Rethink Possible®

Migrating from AT&T DSL service to AT&T U-verse service.

This document is intended as a guide for understanding differences between the two services and specifically some pointers on how to configure your new U-verse Remote Gateway to best fit your previous DSL service.

Two particular subjects covered will be the migrations for Static IP service and from Bridge Mode configurations on DSL.

Some of the Differences

While there are quite a few differences overall between the two services, from the technology to the topology we will cover some of them which can in one way or another more commonly impact you the customer.

- Various means of delivering the "last mile" of service. With your DSL service it is almost all ADSL technology. With **AT&T U-verse** there are various means of connecting to the service. There are VDSL, Fiber and IP-DSL depending on where your home or office is located. Closer in and you are more likely to get service via VDSL, in Apartments or other similar locations you may get service via Fiber, and if you are outside those areas but within ADSL ranges you are more likely to be served by ADSL2+.
- **Authentication** onto the network is different, there is no **PPPoE** authentication on the **AT&T U-verse** network.
- Due to the architecture of the AT&T U-verse platform, Bridge mode is not supported on the network nor on the RG. There will be separate sub-sections dealing with how best to configure the RG for your particular need instead.
- **Ping and Trace** – by default **AT&T U-verse** RG's are set to not respond to ICMP requests such as Ping and Trace. This is configurable through the user interface. Also as the network utilizes MPLS your trace routes will often have lines which time out. This is not an indicator of trouble it is just that that particular hop or node is not set to reply to ICMP requests. This is very much a common policy today as answering ICMP requests adds to CPU utilization and can impact network performance when attacks are made via mass ICMP request attempts commonly referred to as Denial of Service attacks.
- **Use of 10.x.x.x IP addresses** – the DHCP server in the RG is configured not to allow 10.x.x.x IP scope to be set as the DHCP IP addresses. **You may continue to use 10.x.x.x addresses on the LAN side of a 3rd party router** but the RG can not be configured to hand out 10.x.x.x. IP addresses.
- **Static IP delivery** –
  - with your DSL service the DSL modem was often set to bridge mode, one IP address was used at the Access device on our side as the Gateway IP address and minus the Network and Broadcast IP addresses the rest were for users to configure on their equipment with the customer device being the next logical hop out from the Access device. (For those with a single Static IP there is no equivalent in U-verse today.) Also note that you will not be able to keep any existing Static IP addresses. They are a part of a larger block routed for DSL service.
  - With **AT&T U-verse** the RG is now our access device for this scenario. It has its own IP for its WAN which is a sticky dynamically assigned IP. A Virtual port is then created on the LAN side for the Public / Static IP block and like the DSL Access device uses one IP from the block as the Gateway. The remaining are handed to the customer device.
  - A common misconception is that using **DMZplus / IP Passthrough** (depending on device) will completely remove the RG as the firewall and the Gateway. Neither of them are the case in general. Those modes pass the sticky DHCP assigned IP of the RG WAN connection, which is separate from the Static IP block , to the assigned device. Also there is always a portion of the RG's firewall functionality that remains in place by design for our U-verse services. This will be discussed in later sections of the document.

These are some of the differences that are most likely to impact you in your migration.

DMZplus / IP Passthrough

DMZ mode on many home routers and broadband devices bypasses the firewall with an effective any-to-any filter. Meaning any IP or port can go to any IP or port. The intent being to let the assigned device placed into the DMZ handle its own security.

DMZ mode is known as **DMZplus** on the **Pace** RG's 3800, 3801, iNID and newer devices.

DMZ mode is known as **IP Passthrough** on the **Motorola** RG's NVG510 and newer. (**note** – presently IP Passthrough hands off a /32 subnet which does not include the gateway IP and so you should manually / statically assign the IP and subnet mask after it hands it off. A fix for this is scheduled for this.)

For **AT&T U-verse** this is still the general intent but due to some requirements for the U-verse platform even when in these modes there are some situations where the behavior will not be what you expect.

This mode will work well for a user placing a PC in DMZ mode. It will work in many cases for a customer placing their own router in DMZ mode and are not using Static IP's offered by AT&T's Static IP Service.

It is recommended however for consistency or if you are using Static IP's or VPN connections that you not use DMZ mode and instead create firewall rules / pinholes to allow the ports you need for a device. To some extent this can be an any to any rule. More discussion on doing this is included later in the document.

VPN and AT&T U-verse

When using **VPN** across the **AT&T U-verse** platform it is often necessary to lower the **MTU** (Maximum Transmitable Unit) setting of the VPN client or if using a concentrator then the egress port to the **AT&T U-verse** RG to **1472**. Common symptoms of MTU needing to be lowered would be VPN connections not being stable or having very poor performance for applications and browsing that traverses the VPN.

Often lowering the MTU on your end alone will correct this, sometimes it may additionally require adjustment on the far end as well.

Also a note on the **Motorola NVG510** – VPN connections using **PPPTP** or **L2TP** will require setting up the **GRE ALG** option (or PPTP etc) in the NAT/Gaming section.

Now How Do We Configure the RG for these things?

The rest of the document is divided into sections covering the **Pace** devices and separate sections for the **Motorola** devices.

As this will be delivered in a PDF document there will be bookmarks for the sections so you may skip to those applicable to you.

Configuring U-verse Pace devices 3600 / 3800 /3801/5031/5168 and iNID for use with 3rd party Firewall / Router devices.

Pace 3600, 3800, 3801, 5031, 5168 and iNID devices.

This section walks through configuring the PACE RG to work with 3rd Party routers or firewall devices. For those migrating from a DSL or other service which would allow them to put the modem into a “Bridge” mode.

U-verse Platform Gateways (RG's) – Do Not Have a Bridge Mode.

As mentioned earlier in the document the Firewall is never completely out of the picture. Configurations can be made to allow much of the behavior typically needed when using a bridge mode but there may be some limitations for those with more advanced needs.

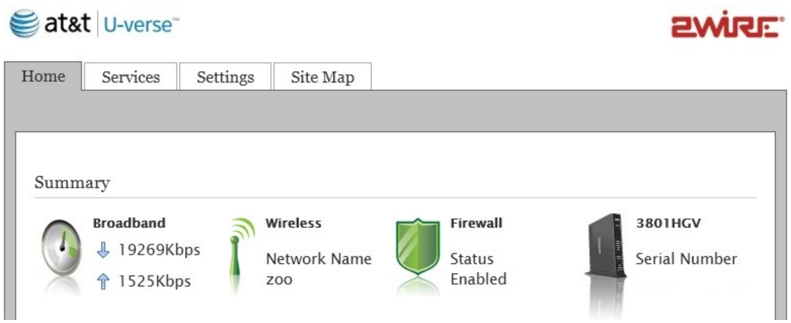
Those limitations can mostly be overcome once the user understands this and is willing / able to adapt how things on the LAN are configured and update. What can be done is based on the need such as Basic service using DMZplus or Static IP service.

For those needing 3rd party routers and or firewall devices between the RG and their network it is better for the U-verse Platform RG's to leave the Firewall enabled and to create pinholes for the traffic that is expected / required to be used. This especially applies to any traffic that could or would be initiated from the WAN side such as a remote location. It is also recommended when applicable to use DHCP IP assignment to the 3rd party Router or Firewall for its connection.

Configuring the 3600, 3800, 3801 or iNID Firewall

Open the RG’s portal page by entering the LAN side IP of the RG (192.168.1.254 is the default private IP.) If using the Static IP block go to the Gateway IP for the block (typically the next to last IP in the block)

You should see a page like this at the top:



Summary

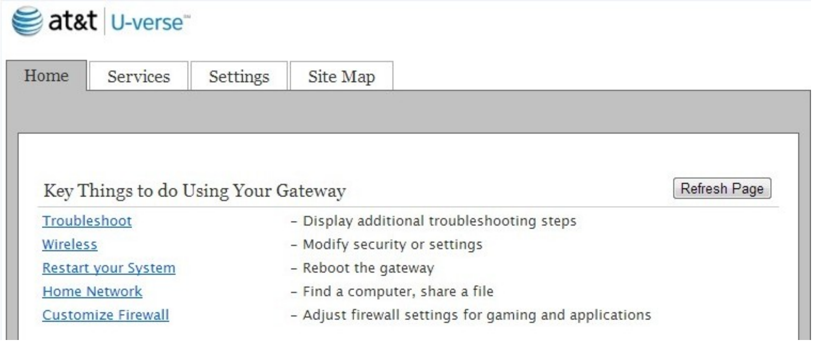
Broadband
19269Kbps
1525Kbps

Wireless
Network Name
zoo

Firewall
Status
Enabled

3801HGV
Serial Number

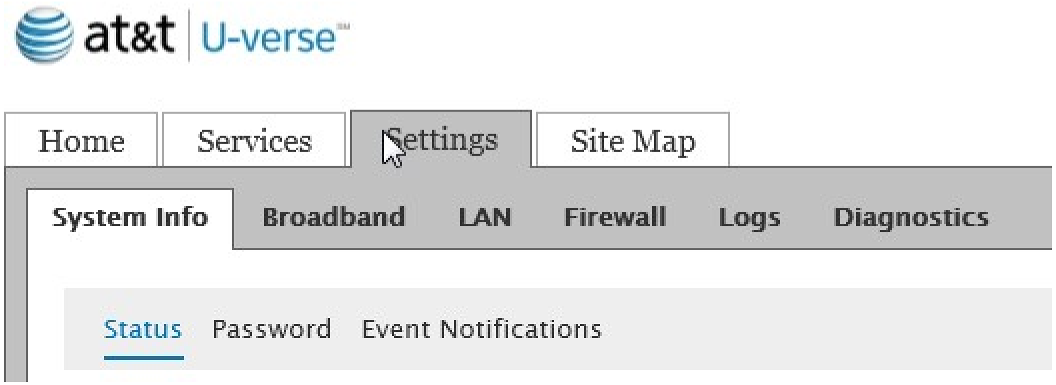
or



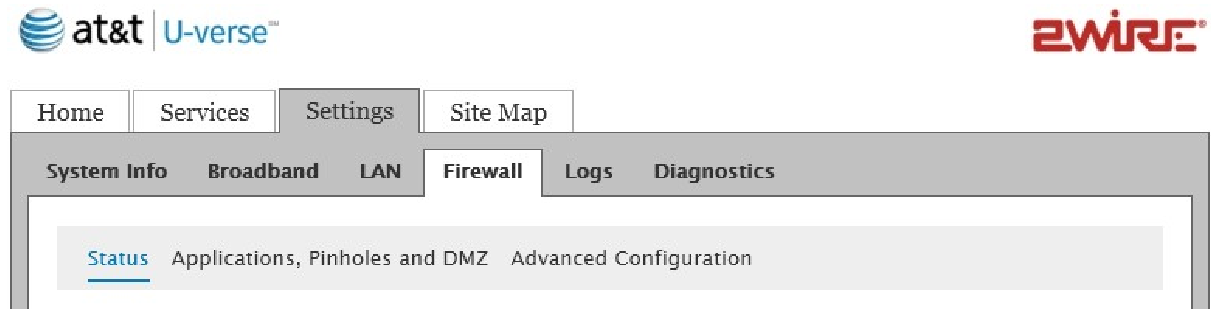
Key Things to do Using Your Gateway

- Troubleshoot – Display additional troubleshooting steps
- Wireless – Modify security or settings
- Restart your System – Reboot the gateway
- Home Network – Find a computer, share a file
- Customize Firewall – Adjust firewall settings for gaming and applications

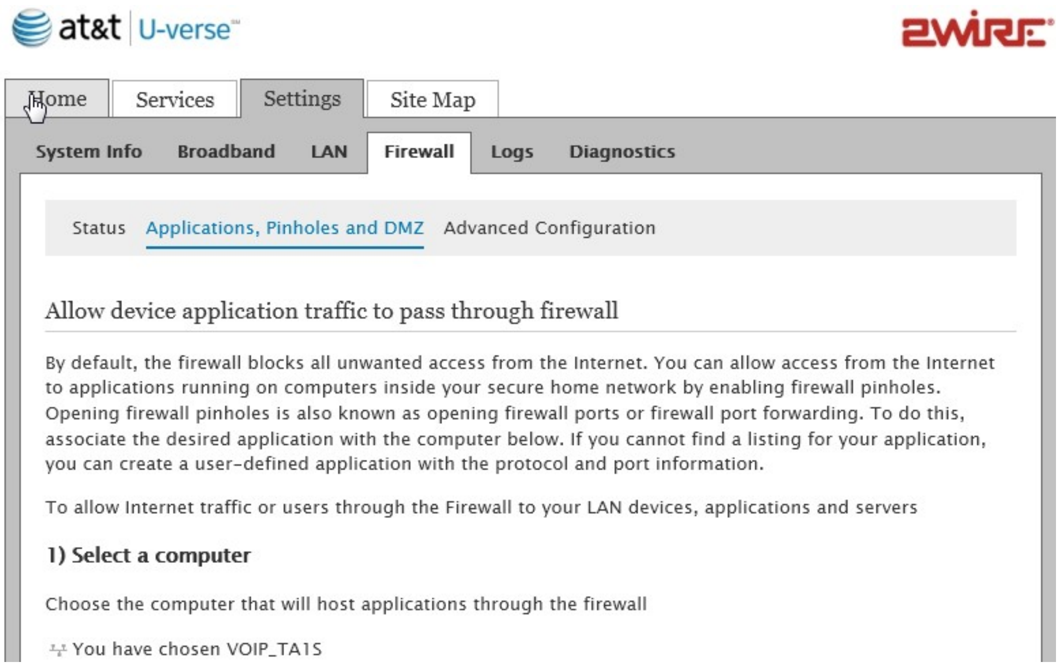
Then go to the Settings tab



Next go to the Firewall option



Select the Applications, Pinholes and DMZ option



Allow device application traffic to pass through firewall

By default, the firewall blocks all unwanted access from the Internet. You can allow access from the Internet to applications running on computers inside your secure home network by enabling firewall pinholes. Opening firewall pinholes is also known as opening firewall ports or firewall port forwarding. To do this, associate the desired application with the computer below. If you cannot find a listing for your application, you can create a user-defined application with the protocol and port information.

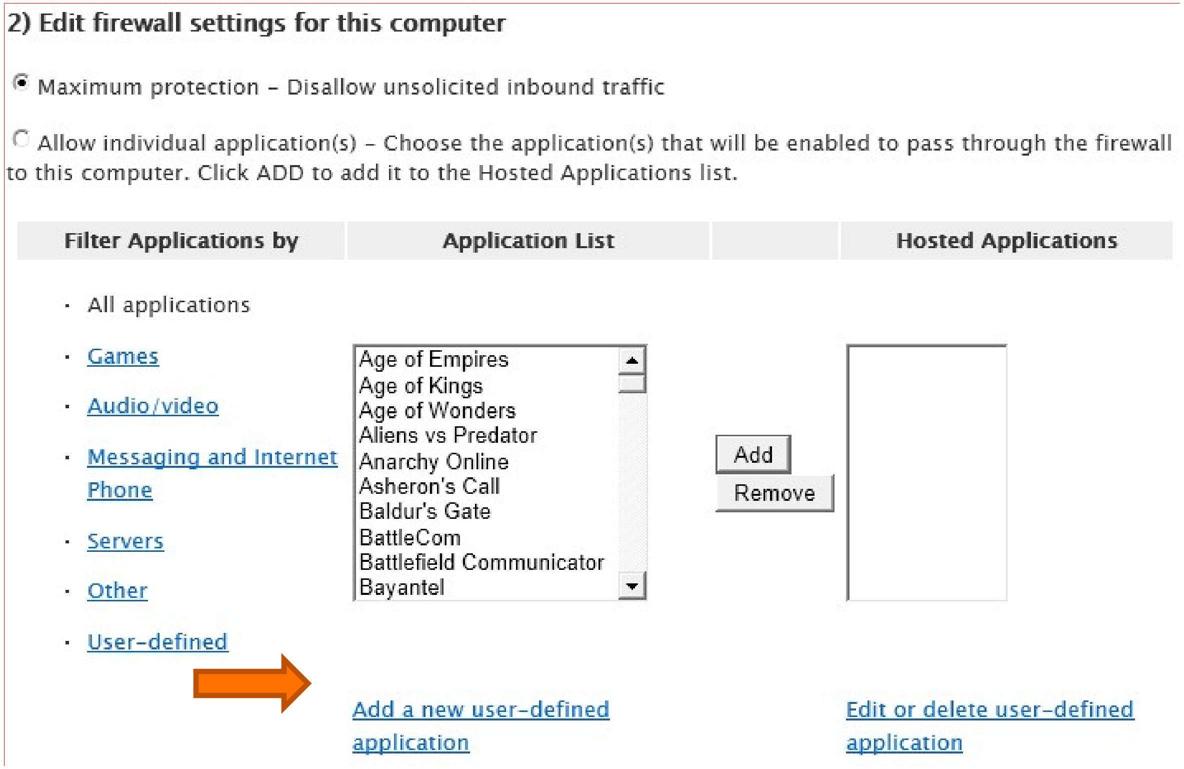
To allow Internet traffic or users through the Firewall to your LAN devices, applications and servers

1) Select a computer

Choose the computer that will host applications through the firewall

You have chosen VOIP_TA1S

Next we will create a new user-defined application (read as rule or template) which we will then apply to the 3rd party Firewall or Router device. Click on the Add a new user-defined application option under the list of existing applications.



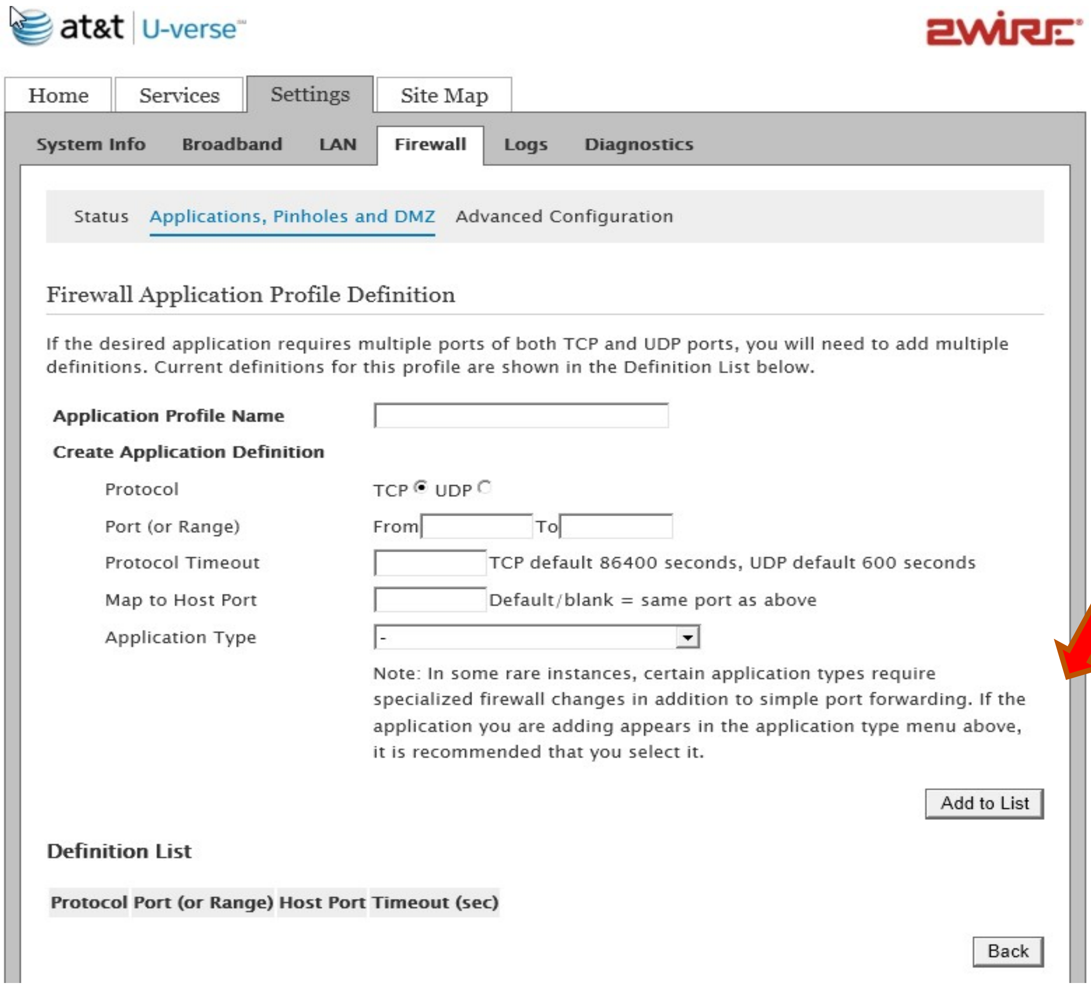
2) Edit firewall settings for this computer

● Maximum protection – Disallow unsolicited inbound traffic

○ Allow individual application(s) – Choose the application(s) that will be enabled to pass through the firewall to this computer. Click ADD to add it to the Hosted Applications list.

Filter Applications by	Application List		Hosted Applications
- All applications - Games - Audio/video - Messaging and Internet Phone - Servers - Other - User-defined	Age of Empires Age of Kings Age of Wonders Aliens vs Predator Anarchy Online Asheron's Call Baldur's Gate BattleCom Battlefield Communicator Bayantel	Add Remove	
	Add a new user-defined application		Edit or delete user-defined application

Next we will enter the ports we need available for this rule or application.



Firewall Application Profile Definition

If the desired application requires multiple ports of both TCP and UDP ports, you will need to add multiple definitions. Current definitions for this profile are shown in the Definition List below.

Application Profile Name

Create Application Definition

Protocol TCP ● UDP ○

Port (or Range) From To

Protocol Timeout TCP default 86400 seconds, UDP default 600 seconds

Map to Host Port Default/blank = same port as above

Application Type -

Note: In some rare instances, certain application types require specialized firewall changes in addition to simple port forwarding. If the application you are adding appears in the application type menu above, it is recommended that you select it.

Definition List

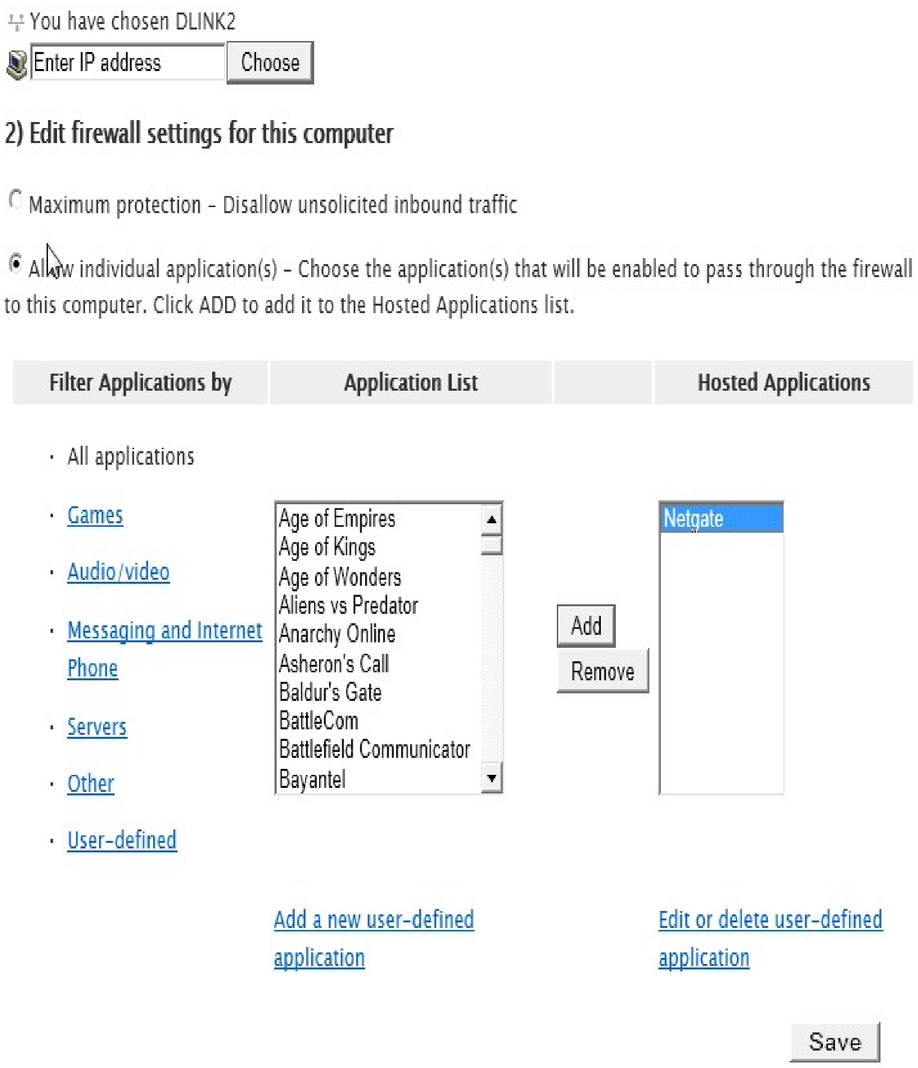
Protocol	Port (or Range)	Host Port	Timeout (sec)

1. Give it an application Name
2. Select TCP or UDP
3. Enter the port range – I typically repeat the port if single. **NOTE** – Although you could specify 0 to 65000 or the highest port number to achieve an effective ANY ANY – the Pace device will not allow you to save it in that manner. You will need to leave some for its own use. So you will need to break it up into 2 or more and leave some available for the RG's own use.
4. Protocol timeout can be left for default.
5. Map to Host Port can be left for default
6. Application type is to let the RG know if the port is for a particular kind of service that it needs to handle separately from its own services. Some of those listed are for DNS, SIP, FTP and few others.
7. Click Add to List
8. The area under Definition List will list the sub rules you have Added for this App.
9. Repeat for each port / port range needed.

   So you would have 1 rule for each port you need in particular for traffic that is or could be initiated remotely and for each port as separate rule for TCP and UDP as needed.

   Once you have added all of them click the back button. This will save the application definition with all entries in this case to the name you gave it.

Next we will apply the custom rule.



You have chosen DLINK2

Enter IP address | Choose

2) Edit firewall settings for this computer

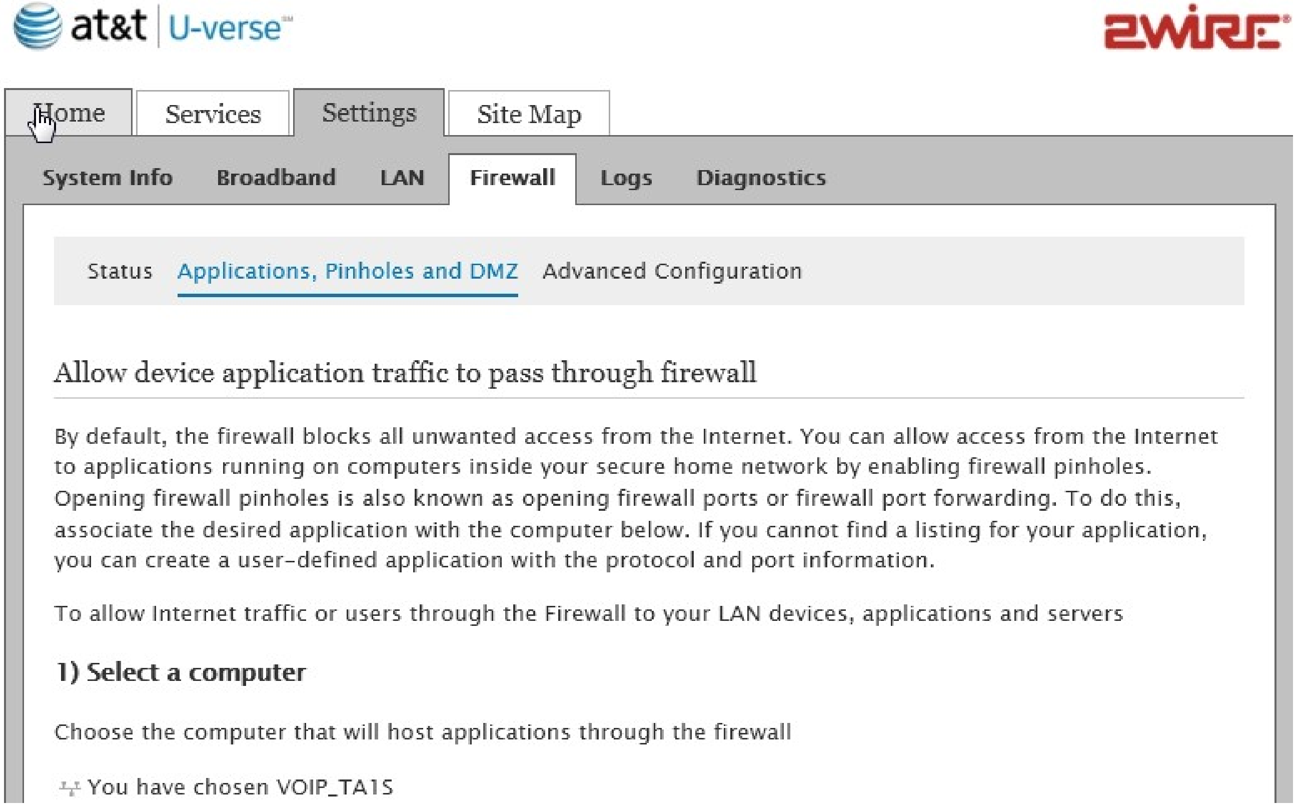
○ Maximum protection - Disallow unsolicited inbound traffic

● Allow individual application(s) - Choose the application(s) that will be enabled to pass through the firewall to this computer. Click ADD to add it to the Hosted Applications list.

Filter Applications by	Application List		Hosted Applications
- All applications - Games - Audio/video - Messaging and Internet Phone - Servers - Other - User-defined	Age of Empires Age of Kings Age of Wonders Aliens vs Predator Anarchy Online Asheron's Call Baldur's Gate BattleCom Battlefield Communicator Bayantel	Add Remove	Netgate
	Add a new user-defined application		Edit or delete user-defined application

1. First you will need to Select the device you are applying the rule to. (from the list near the top.) Once you have selected it it will show You have chosen it. (NOTE – it is better to assign rules to Devices rather than to IP addresses. This way if for any reason the IP address of the device changes the rule will still work. So for example if for some reason the Public IP block stops working the private IP could be used and no changes to the rule would be required.)
2. Select **Allow Individual applications**
3. Scroll through the list of Applications in the Application List box and select the rule you just created.
4. Click the **Add** button to the right of the list between the columns.
5. It will now appear in the **Hosted Applications** list.
6. Click the **Save** button further down the page on the right.
7. This has now applied the rule.

To verify it is applied at the top of the page where the Firewall tab is select the Status option.



Allow device application traffic to pass through firewall

By default, the firewall blocks all unwanted access from the Internet. You can allow access from the Internet to applications running on computers inside your secure home network by enabling firewall pinholes. Opening firewall pinholes is also known as opening firewall ports or firewall port forwarding. To do this, associate the desired application with the computer below. If you cannot find a listing for your application, you can create a user-defined application with the protocol and port information.

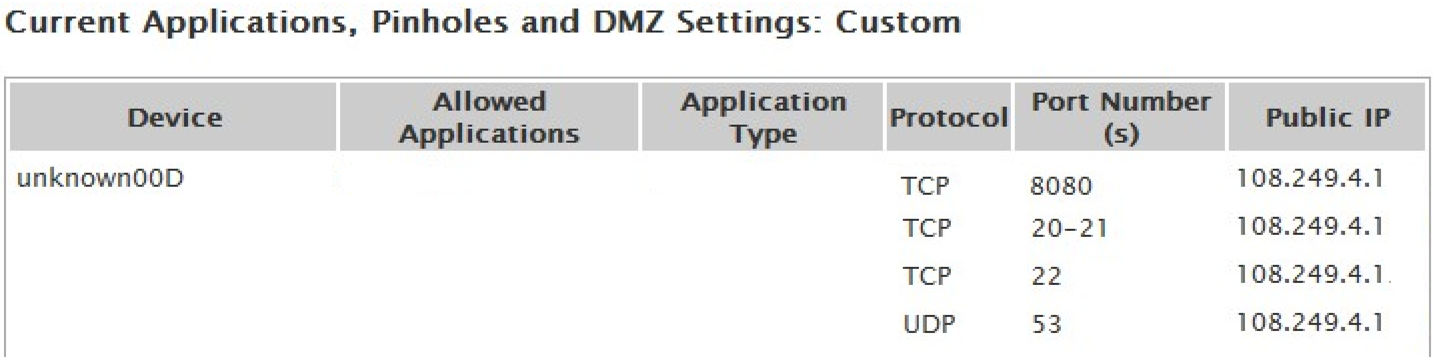
To allow Internet traffic or users through the Firewall to your LAN devices, applications and servers

1) Select a computer

Choose the computer that will host applications through the firewall

You have chosen VOIP_TA1S

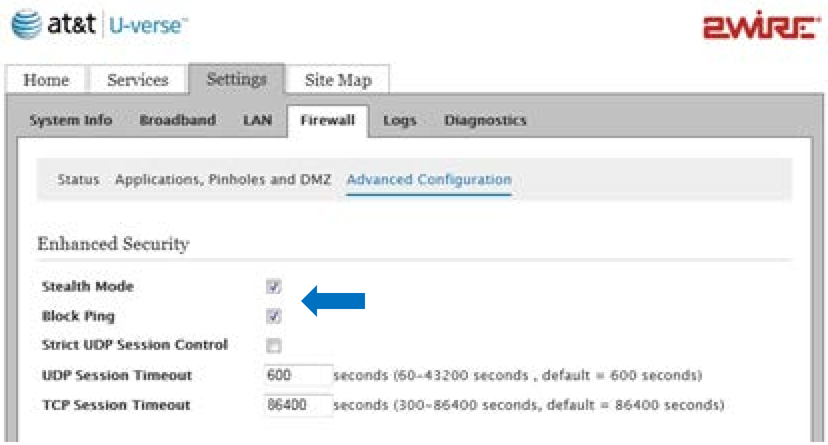
You should now see something like the following. Do not worry about the Application Type not reflecting the FTP portion – it is because this has multiple definitions within the one Application rule.



Current Applications, Pinholes and DMZ Settings: Custom

Device	Allowed Applications	Application Type	Protocol	Port Number (s)	Public IP
unknown00D			TCP	8080	108.249.4.1
			TCP	20-21	108.249.4.1
			TCP	22	108.249.4.1
			UDP	53	108.249.4.1

Firewall – Advanced Settings – Allowing Ping



Enhanced Security

Stealth Mode	☑	
Block Ping	☑	
Strict UDP Session Control	□	
UDP Session Timeout	600	seconds (60-43200 seconds , default = 600 seconds)
TCP Session Timeout	86400	seconds (300-86400 seconds, default = 86400 seconds)

By default the U-verse RG does not reply to Ping or Trace and does not allow those to be passed thru the firewall from the WAN side.

To enable Ping and Trace two settings must be changed. This can be done on the Settings / Firewall / Advanced Configuration page

Stealth Mode – Remove the check mark. This settings by default means the RG does not itself respond to ICMP queries.

Block Ping – Remove the check mark. This setting is what will allow Ping and Trace commands through the firewall from the LAN side.

NOTE – at this time the consistency of the replies even with these settings will vary.

A note about ping and trace – the standard form of IP Ping and Trace use ICMP requests.

ICMP requests are quite often not answered or answered with a very low priority. Actual data traversing the same hop has a higher priority and does not experience the same delay. So for example in a trace today you may see time outs but the trace completes. The time outs do not indicate a problem but instead indicate only that those hops are configured not to reply to ICMP requests. Also if the destination device is set to not reply then a ping or trace can time out and still not be an accurate indicator of if there is a problem.

This is mentioned to keep in mind not to use this as your only or even primary trouble indicator.

Configuring Static IP

This Section will walk you through configuring the RG for use of a Static IP block. As mentioned earlier but repeated here for convienianсe is an overview in differences between ADSL service handling of Static IP service and AT&T U-verse

- **Static IP delivery –**
  - with your DSL service the DSL modem was often set to bridge mode, one IP address was used at the Access device on our side as the Gateway IP address and minus the Network and Broadcast IP addresses the rest were for users to configure on their equipment with the customer device being the next logical hop out from the Access device.
  - With AT&T U-verse the RG is now our access device for this scenario. It has its own IP for its WAN which is a sticky dynamically assigned IP. A Virtual port is then created on the LAN side for the Public / Static IP block and like the DSL Access device uses one IP from the block as the Gateway. The remaining are handed to the customer device.
  - A reason this is different is that the Static IP block is routed to the WAN IP (dynamically assigned) of the RG and mapped to the MAC address of the RG for anti-spoofing purposes.
  - The common misconception is that using DMZplus / IP Passthrough (depending on device) will completely remove the RG as the firewall and the Gateway. Neither of them are the case in general. Those modes pass the sticky DHCP assigned IP of the RG WAN connection, which is separate from the Static IP block , to the assigned device. Also there is always a portion of the RG's firewall functionality that remains in place by design for our U-verse services. This will be discussed in later sections of the document.

Enable Public Routed Sub-interface

This section would have been completed by the U-verse installer and is provided here for reference to verify it is configured as suggested. Also in case of a factory reset where it is required to be reconfigured.

1. Determine the Public IP block information to configure in the Residential Gateway. (example x.x.x.x /29)

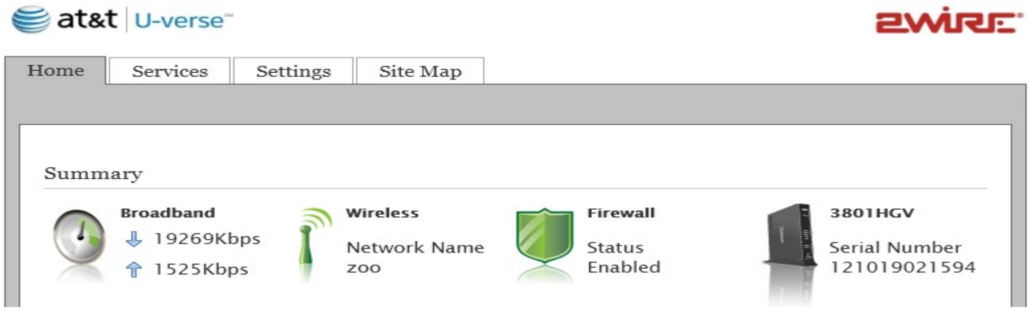
The RG will use two sets of Public IP addresses, one IP for use between the router and the broadband network (WAN side)and a second independent set of Public Static IP addresses solely for use on the LAN side.   The WAN side IP is a Dynamically assigned IP address that is “sticky” It should change only under certain conditions. Some of those conditions are

- The RG is replaced by another RG
- The VDSL port is swapped at the DSLAM
- The RG is offline for an extended time which could then fail to renegotiate its IP lease.

The Public / Static IP block will be dynamically mapped and routed to the WAN IP and a single IP out of the block will be assigned to a virtual port on the LAN side of the RG. That IP will be the gateway for the rest of the devices using the Static IP block behind the RG. Typically we use the next to last IP in the block for this Gateway IP.

Log into the RG GUI page by putting in the gateway IP (192.168.1.254 is default address.)

You should see the opening screen of the portal with something like this.



Summary

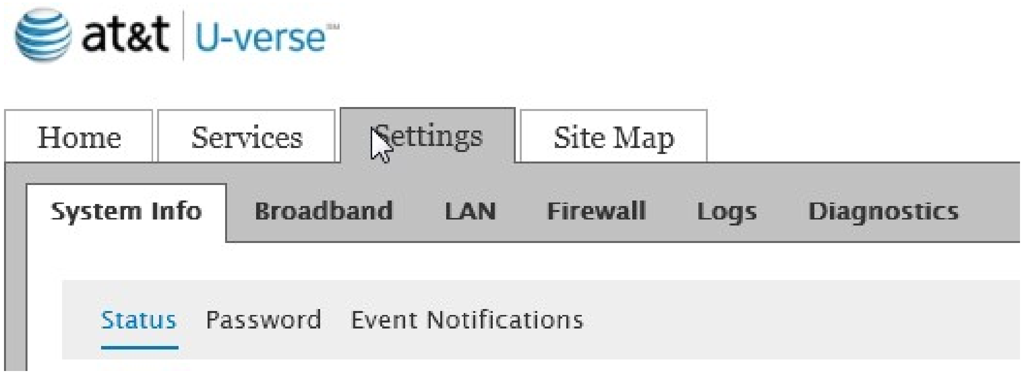
Broadband
19269Kbps
1525Kbps

Wireless
Network Name
zoo

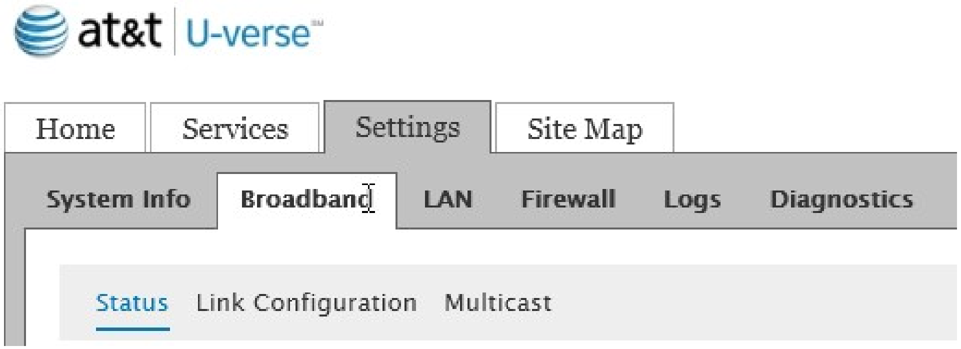
Firewall
Status
Enabled

3801HGV
Serial Number
121019021594

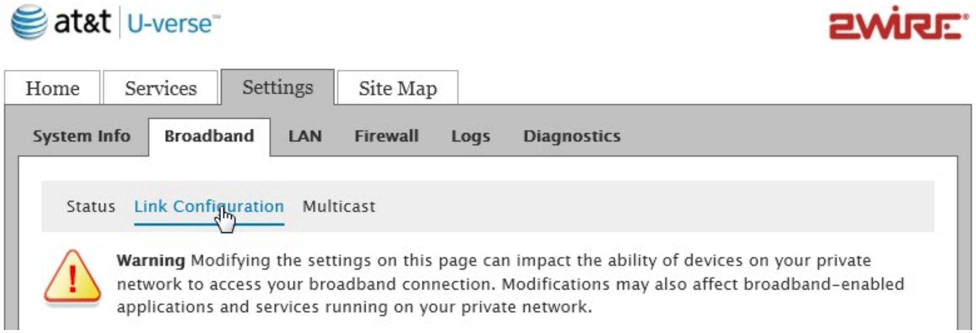
Then click on the Settings tab which will bring you to a page like this:



Now click on the Broadband

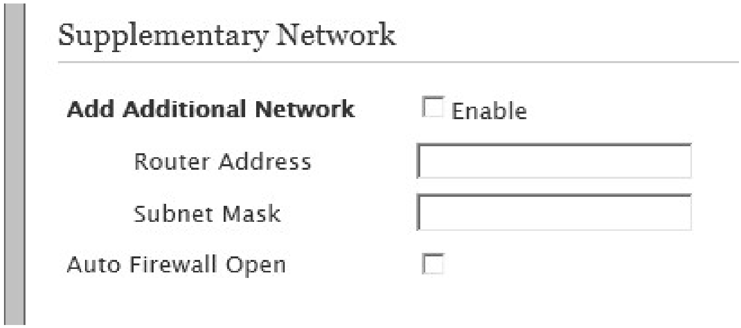


Click on the Link Configuration option.



Warning Modifying the settings on this page can impact the ability of devices on your private network to access your broadband connection. Modifications may also affect broadband-enabled applications and services running on your private network.

Go to the Supplementary Network section near the bottom of the page.



Supplementary Network

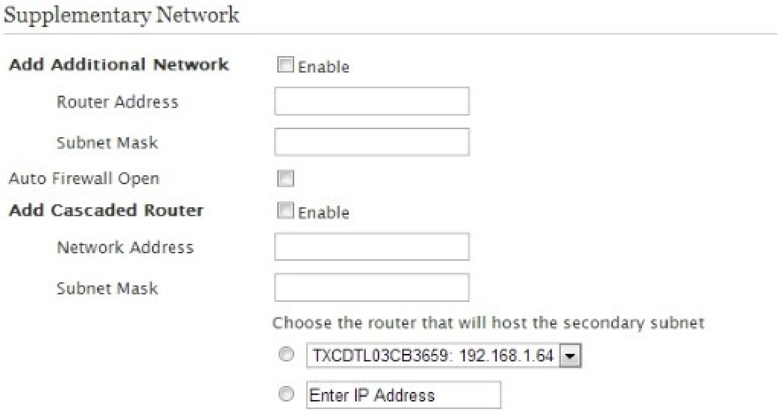
Add Additional Network □ Enable

Router Address

Subnet Mask

Auto Firewall Open □

or



Supplementary Network

Add Additional Network □ Enable

Router Address

Subnet Mask

Auto Firewall Open □

Add Cascaded Router □ Enable

Network Address

Subnet Mask

Choose the router that will host the secondary subnet

○ TXCDTL03CB3659: 192.168.1.64

○ Enter IP Address

The Add Additional Network box for Enable should be checked.

The Router Address will be one of the available IPs from the Static / Public block issued. Typically this would be the next to the last IP in the block but the 2nd one is another common one. The Subnet Mask should be set to 255.255.255.x where x depends on the amount of IP addresses you have. Start with 255 and subtract the number of IP addresses in your block and that will be the subnet value for x. For example 8 IPs would be 248

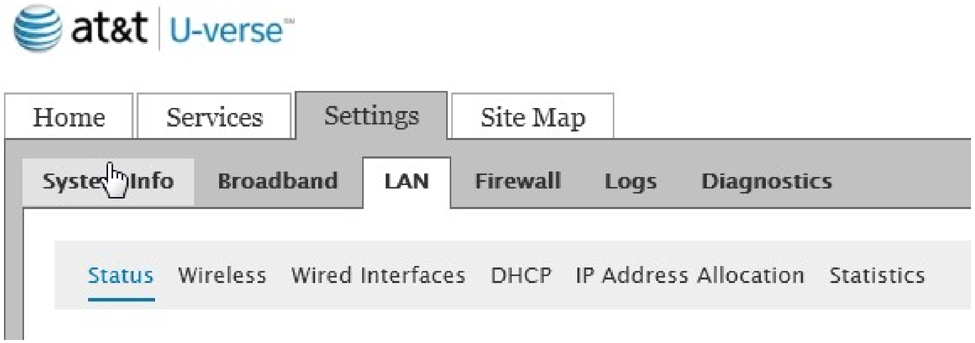
The Auto Firewall Open box should be checked. This in particular applies to connection requests generated by devices on the LAN and using one of the Static IP addresses. Rules should still be made for connection requests or traffic originating on the WAN / Internet side of things. We will cover how that works later.

Some devices and firmware also support Cascaded Router.

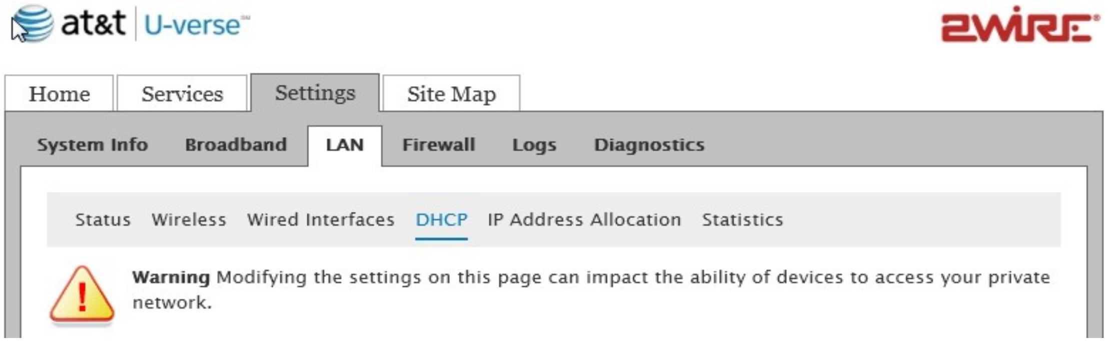
This option allows the RG to route the entire Public IP block over to a particular device or IP address. Think of it as a next hop situation. In this mode the RG does not reserve one of the Public IP addresses for a virtual interface, instead it is configured to route any IP addresses in the configured block over to the specific device or private IP address. The destination router then would use, hand out via DHCP and route the Public IP block.

To enable Cascaded Router place a check in the Enable box next to it. Then add in the Public IP block in the Network Address and the Subnet Mask. Then choose the radio button for either the device and select the device in the drop down menu or select and enter the IP private IP address of the device you will route to.

Next go to the LAN tab

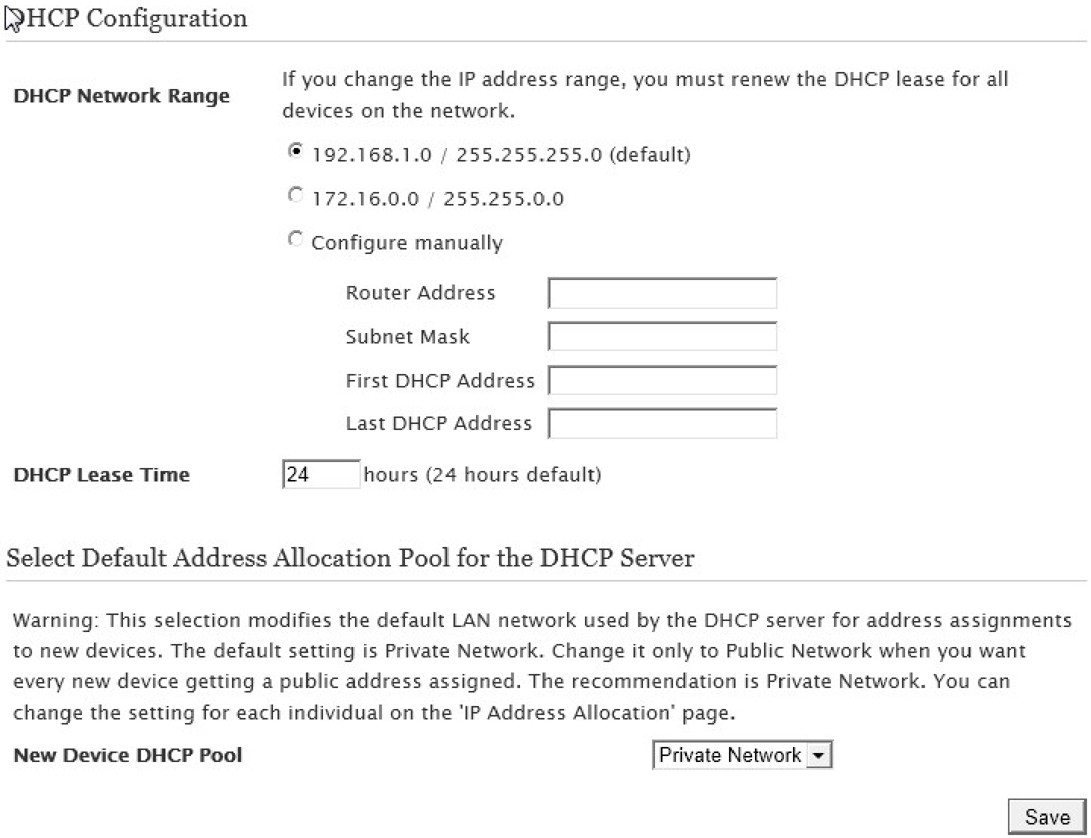


Click on the DHCP



Warning Modifying the settings on this page can impact the ability of devices to access your private network.

This section is to verify what DHCP scope or range you wish the RG to use by default (you can assign manually in another section but this would be which it uses by default. You can select Private Network or Public Network if the Public Interface and block information has been configured. Click Save if you have changed anything. **NOTE - if you used Cascaded Router configuration - this step does not apply.**



DHCP Configuration

DHCP Network Range

If you change the IP address range, you must renew the DHCP lease for all devices on the network.

● 192.168.1.0 / 255.255.255.0 (default)

○ 172.16.0.0 / 255.255.0.0

○ Configure manually

Router Address

Subnet Mask

First DHCP Address

Last DHCP Address

DHCP Lease Time 24 hours (24 hours default)

Select Default Address Allocation Pool for the DHCP Server

Warning: This selection modifies the default LAN network used by the DHCP server for address assignments to new devices. The default setting is Private Network. Change it only to Public Network when you want every new device getting a public address assigned. The recommendation is Private Network. You can change the setting for each individual on the 'IP Address Allocation' page.

New Device DHCP Pool Private Network

Configuring U-verse Arris NVG510 or NVG589 for use with 3rd party Firewall / Router devices.

This section walks through configuring the Arris NVG510 or NVG589 RG to work with 3rd Party routers or firewall devices. For those migrating from a DSL or other service which would allow them to put the modem into a "Bridge" mode.

U-verse Platform Gateways (RG's) – Do Not Have a Bridge Mode.

As mentioned earlier in the document the Firewall is never completely out of the picture. Configurations can be made to allow much of the behavior typically needed when using a bridge mode but there may be some limitations for those with more advanced needs.

Those limitations can mostly be overcome once the user understands this and is willing / able to adapt how things on the LAN are configured and update. What can be done is based on the need such as Basic service using **IPPassthrough** or Static IP service.

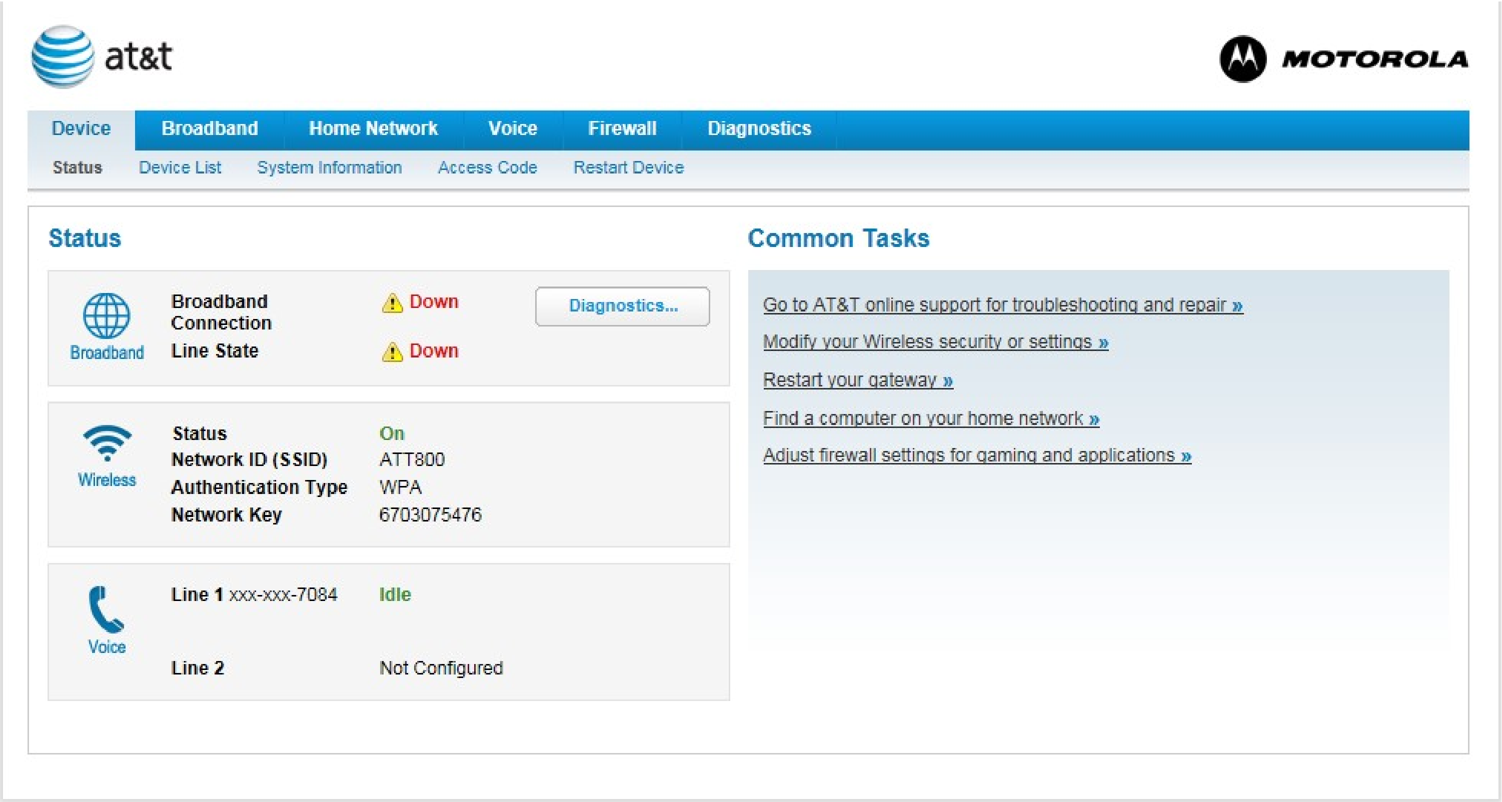
For those needing 3rd party routers and or firewall devices between the RG and their network it is better for the U-verse Platform RG's to leave the Firewall enabled and to create pinholes for the traffic that is expected / required to be used. This especially applies to any traffic that could or would be initiated from the WAN side such as a remote location. It is also recommended when applicable to use DHCP IP assignment to the 3rd party Router or Firewall for its connection.

The **Arris NVG510** or **NVG589** offers a little more choices in the Firewall configuration, this section will include screenshots of these pages and a brief description of their use in general along with a general walk thru of configuring the NAT / Gaming section which is where the pinhole recommendation would be configured.

Configuring the Arris NVG510 or NVG589 Firewall

Open the RG's portal page by entering the LAN side IP of the RG (192.168.1.254 is the default private IP.) If using the Static IP block go to the Gateway IP for the block (typically the next to last IP in the block)

You should see a page like this:



Status

Broadband	Broadband Connection	⚠ Down
	Line State	⚠ Down
Wireless	Status	On
	Network ID (SSID)	ATT800
	Authentication Type	WPA
	Network Key	6703075476
Voice	Line 1 xxx-xxx-7084	Idle
	Line 2	Not Configured

Common Tasks

Go to AT&T online support for troubleshooting and repair »

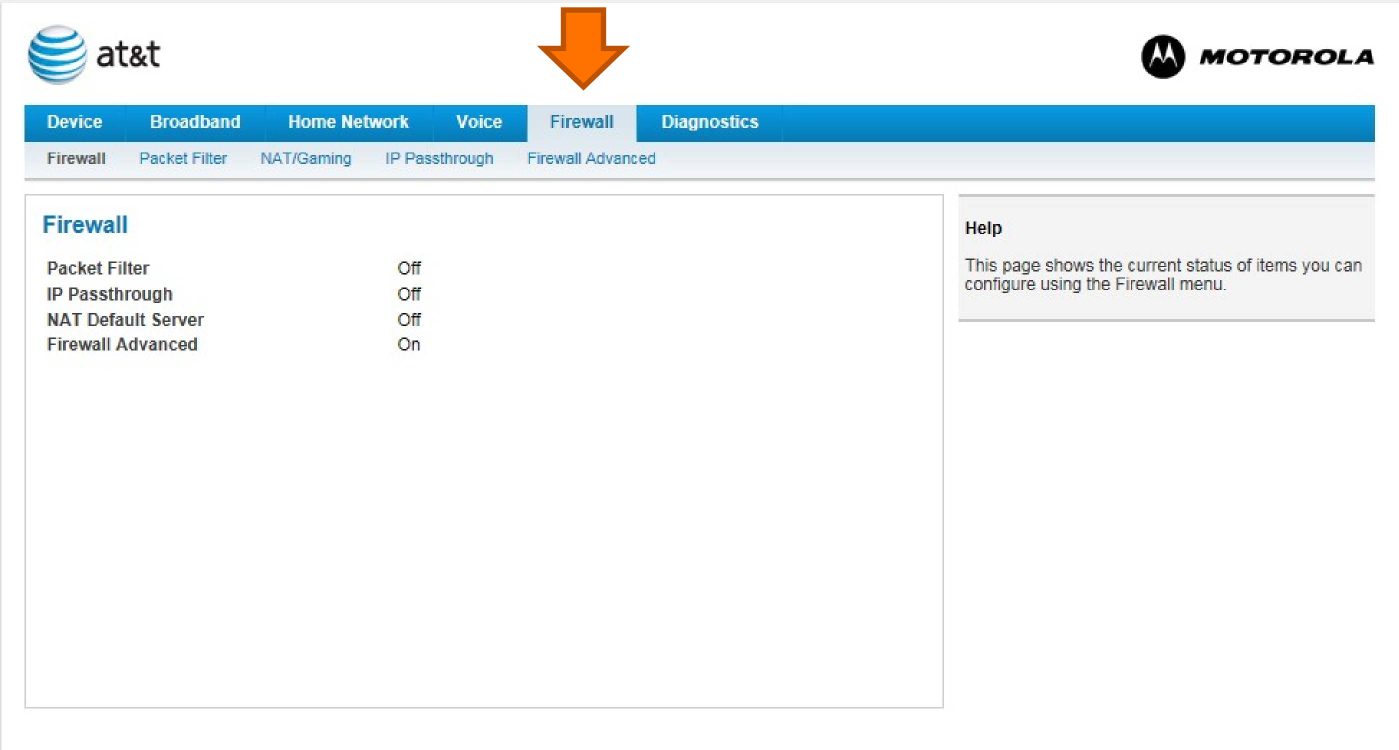
Modify your Wireless security or settings »

Restart your gateway »

Find a computer on your home network »

Adjust firewall settings for gaming and applications »

Click on the Firewall tab. This will bring you to the status page.



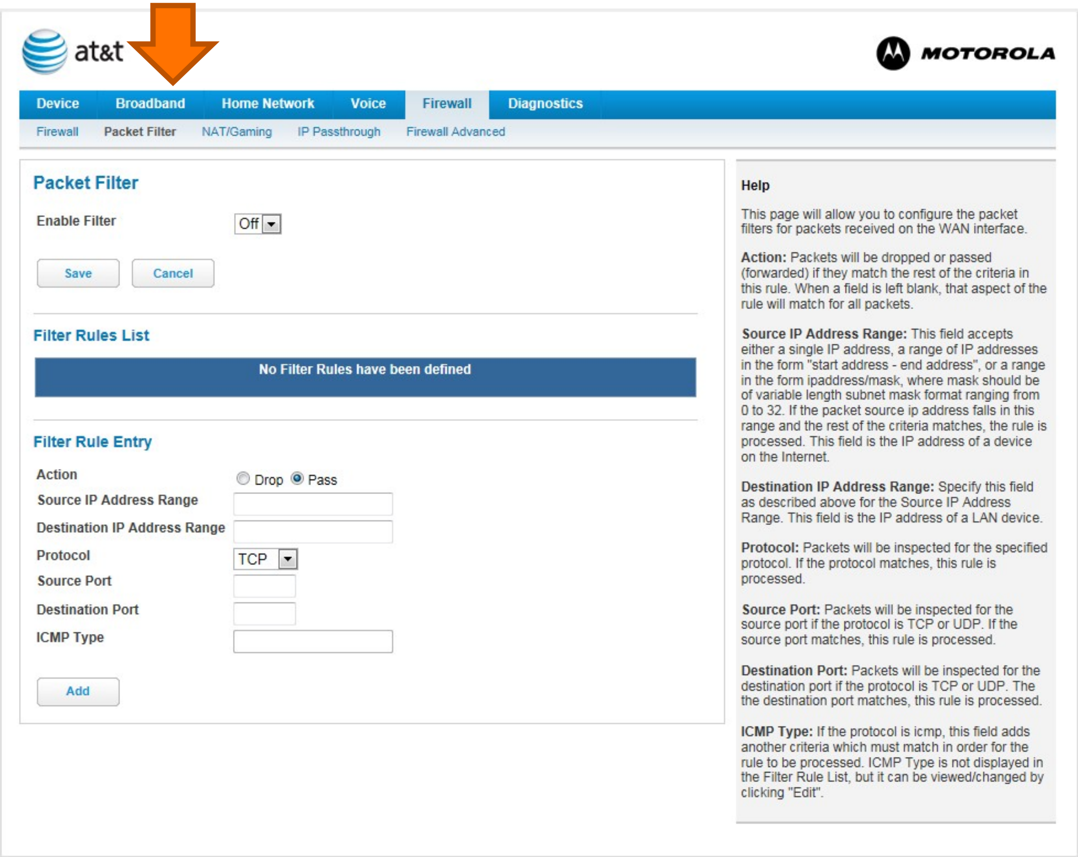
Firewall

Packet Filter	Off
IP Passthrough	Off
NAT Default Server	Off
Firewall Advanced	On

Help

This page shows the current status of items you can configure using the Firewall menu.

Click on the **Packet Filter** tab.



Packet Filter

Enable Filter: Off

Save | Cancel

Filter Rules List

No Filter Rules have been defined

Filter Rule Entry

Action: ○ Drop ● Pass

Source IP Address Range

Destination IP Address Range

Protocol: TCP

Source Port

Destination Port

ICMP Type

Add

Help

This page will allow you to configure the packet filters for packets received on the WAN interface.

Action: Packets will be dropped or passed (forwarded) if they match the rest of the criteria in this rule. When a field is left blank, that aspect of the rule will match for all packets.

Source IP Address Range: This field accepts either a single IP address, a range of IP addresses in the form "start address - end address", or a range in the form ipaddress/mask, where mask should be of variable length subnet mask format ranging from 0 to 32. If the packet source ip address falls in this range and the rest of the criteria matches, the rule is processed. This field is the IP address of a device on the Internet.

Destination IP Address Range: Specify this field as described above for the Source IP Address Range. This field is the IP address of a LAN device.

Protocol: Packets will be inspected for the specified protocol. If the protocol matches, this rule is processed.

Source Port: Packets will be inspected for the source port if the protocol is TCP or UDP. If the source port matches, this rule is processed.

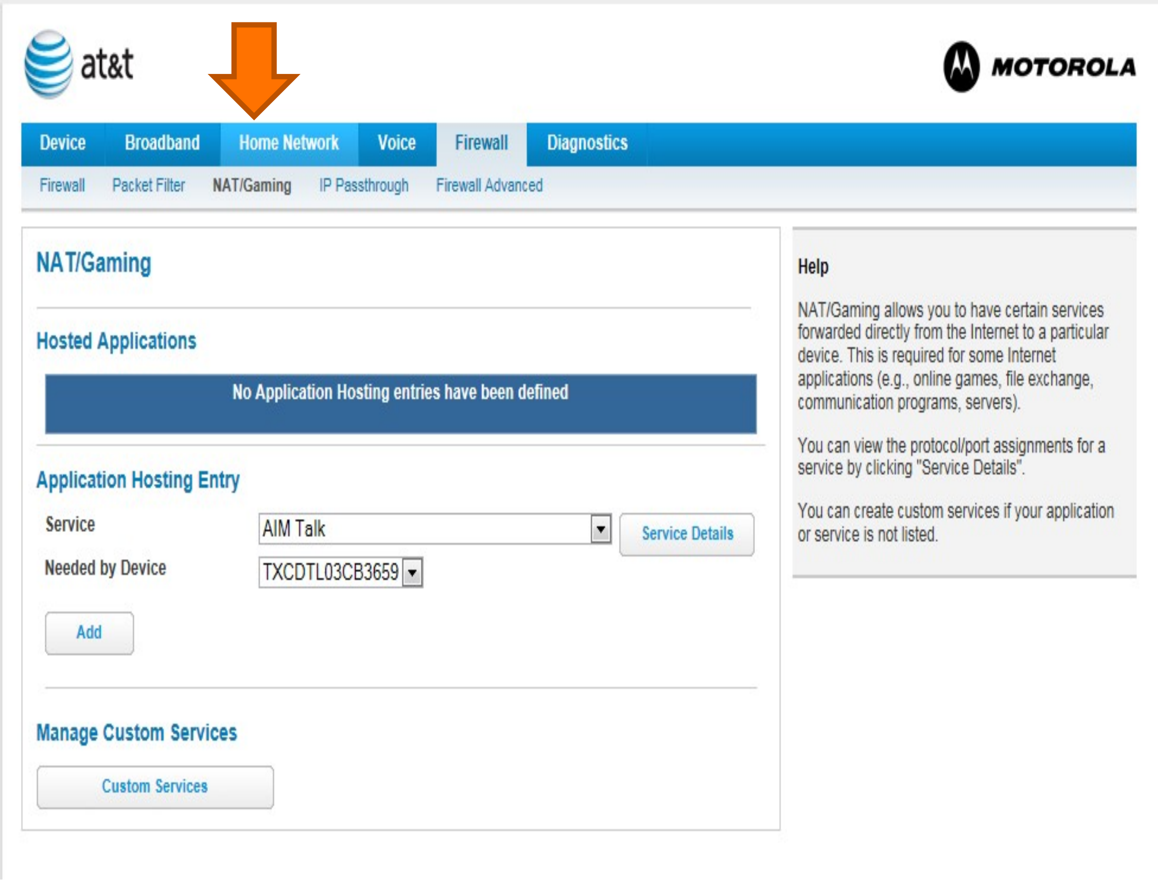
Destination Port: Packets will be inspected for the destination port if the protocol is TCP or UDP. The the destination port matches, this rule is processed.

ICMP Type: If the protocol is icmp, this field adds another criteria which must match in order for the rule to be processed. ICMP Type is not displayed in the Filter Rule List, but it can be viewed/changed by clicking "Edit".

This tab is for those situations where **Packet Filtering** is needed. For instance if you have a range of IP addresses to allow traffic to or from rather than a singe IP on the LAN side or from the LAN to an IP or IP range to allow traffic to.

Where the **NAT/Gaming** will be to allow an identified port to a single device or IP.

Click on the **NAT/Gaming** tab.



NAT/Gaming

Hosted Applications

No Application Hosting entries have been defined

Application Hosting Entry

Service: AIM Talk — Service Details

Needed by Device: TXCDTL03CB3659

Add

Manage Custom Services

Custom Services

Help

NAT/Gaming allows you to have certain services forwarded directly from the Internet to a particular device. This is required for some Internet applications (e.g., online games, file exchange, communication programs, servers).

You can view the protocol/port assignments for a service by clicking "Service Details".

You can create custom services if your application or service is not listed.

This tab is for those situations where a **NAT/Gaming** pinhole is needed.

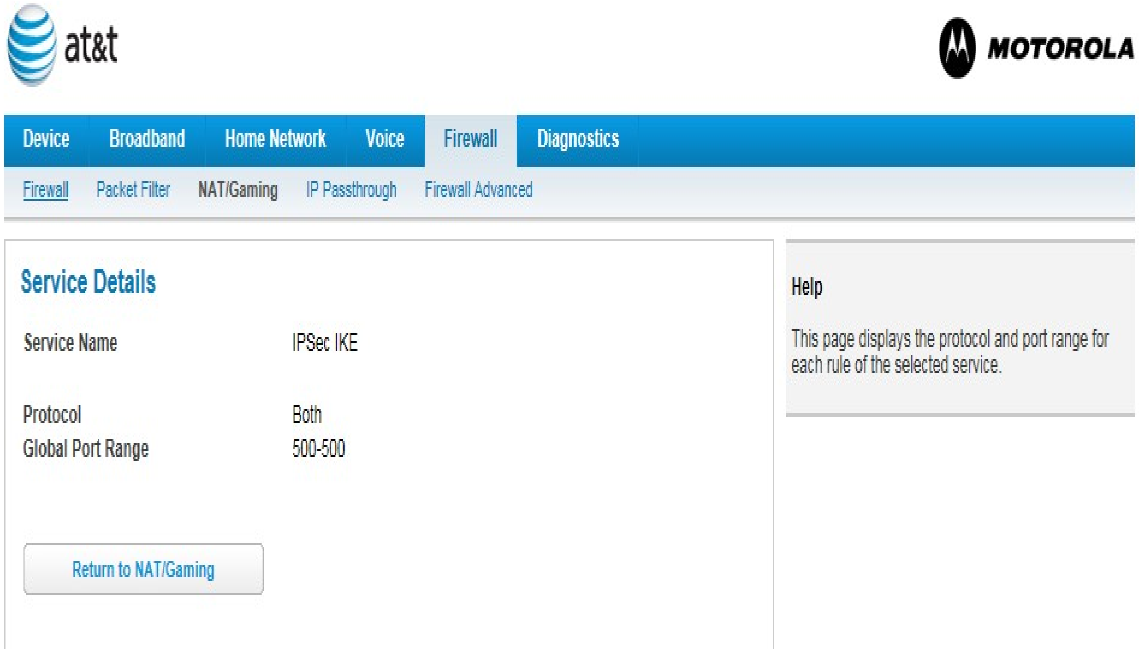
An example is for passing traffic through to a Firewall / VPN / Router device as a single handoff from the **Arris RG or modem.**

In the **Application Hosting Entry** section there are a number of commonly defined applications you may select from. Be sure to use the **Service Details** button to verify the port ranges defined match your particular need for the app.

If you need to or prefer to define you own rule for each port or application you may use the Custom Services section.

We will walk thru **Custom Services** creation further on.

The Service Details button.



Service Details

Service Name IPSec IKE

Protocol Both

Global Port Range 500-500

Return to NAT/Gaming

Help

This page displays the protocol and port range for each rule of the selected service.

This is an example of the **Service Details** page.

Here you will see the **Service Name** / the custom name you gave a rule.

It lists **Protocol** (TCP, UDP, or both)

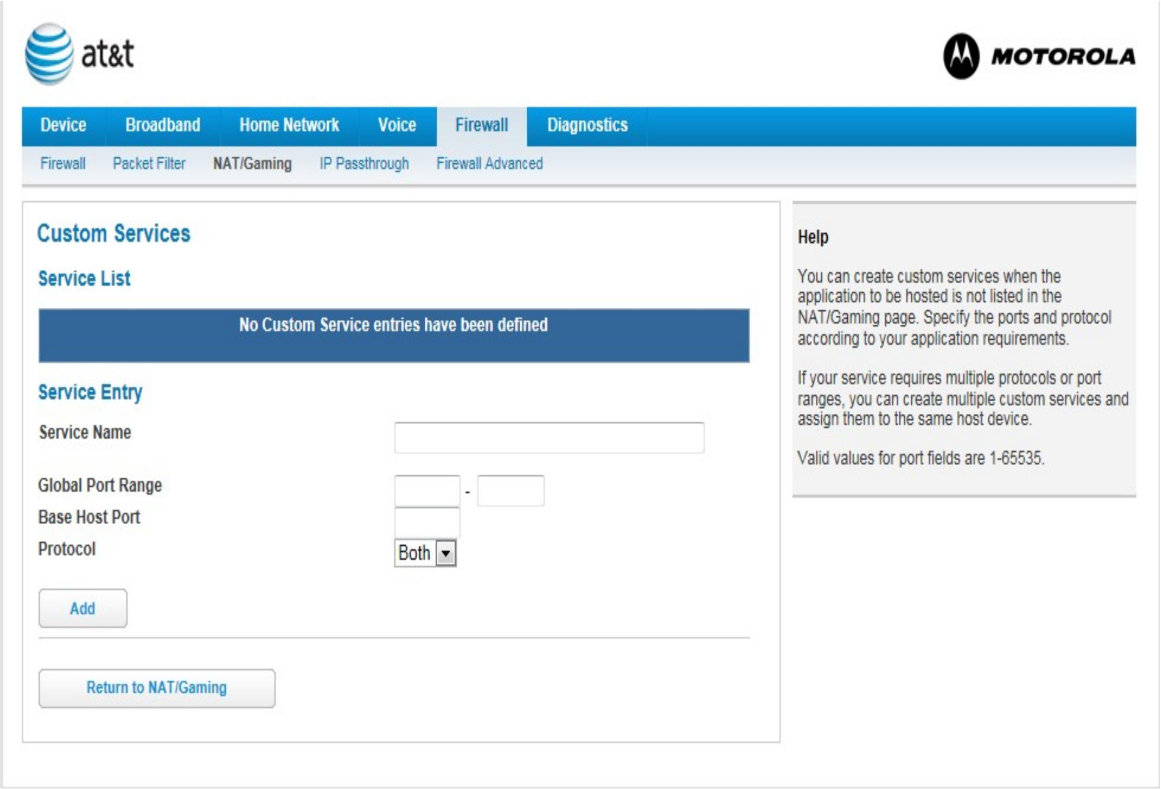
It also lists the **Global Port Range** you want to have opened.

So for the pre-defined rules they use the common ports used for those services. But your own needs may call for different ones.

So just be sure to see what is being used.

NOTE – there are pre-defined services for **IPSec – IKE** as well as for **PPTP** which can be helpful for VPN usage.

The Custom Services button.



Custom Services

Service List

No Custom Service entries have been defined

Service Entry

Service Name

Global Port Range -

Base Host Port

Protocol Both

Add

Return to NAT/Gaming

Help

You can create custom services when the application to be hosted is not listed in the NAT/Gaming page. Specify the ports and protocol according to your application requirements.

If your service requires multiple protocols or port ranges, you can create multiple custom services and assign them to the same host device.

Valid values for port fields are 1-65535.

This is an example of the **Custom Services** page.

Here you will see the Service List which will display the services you define once you add them.

The Service Entry area is where you define you custom rule.

Service Name – give it a custom name – typically the name of the app or service that uses this port.

Global Port Range – give a beginning and ending port range. If a single port then place in both.

Base Host Port the same port as above typically.

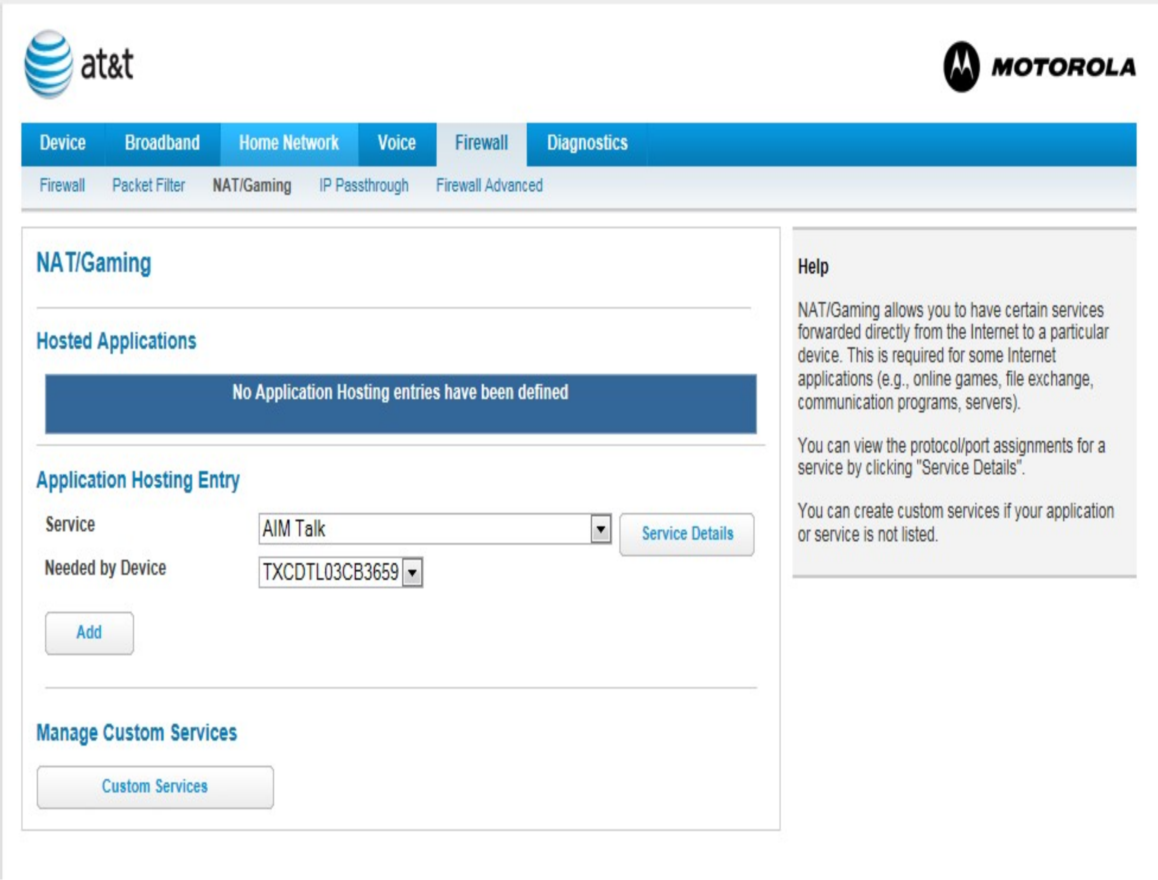
Protocol – select TCP, UDP or Both

Click Add

This will then show the definition in the Service List Box.

Click on Return to NAT/Gaming to continue.

Returned to the **NAT/Gaming** tab.



NAT/Gaming

Hosted Applications

No Application Hosting entries have been defined

Application Hosting Entry

Service: AIM Talk

Service Details

Needed by Device: TXCDTL03CB3659

Add

Manage Custom Services

Custom Services

Help

NAT/Gaming allows you to have certain services forwarded directly from the Internet to a particular device. This is required for some Internet applications (e.g., online games, file exchange, communication programs, servers).

You can view the protocol/port assignments for a service by clicking "Service Details".

You can create custom services if your application or service is not listed.

Now that you have created a custom services rule.

Click on the drop down box for Service and find the new custom service definition you created.

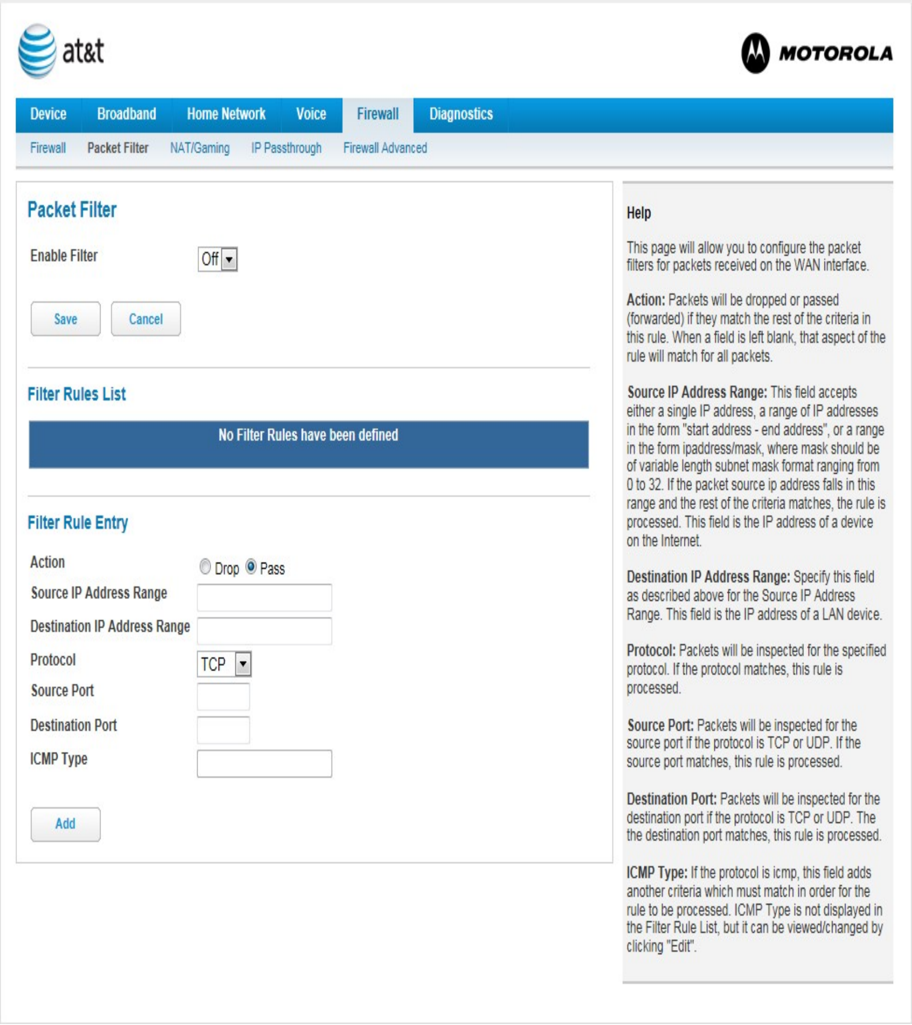
Then click on the drop down box next to Needed by Device and select the device you wish to apply it to such as your PC, Router, Firewall or VPN appliance.

Click Add

This should now show that custom service above in the Hosted Applications section.

Remember you will have to apply a rule custom or otherwise for each port / service you will need open to that device.

Firewall – Allowing Ping and Trace



Packet Filter

Enable Filter: Off

Filter Rules List

No Filter Rules have been defined

Filter Rule Entry

Action	○ Drop ● Pass
Source IP Address Range	
Destination IP Address Range	
Protocol	TCP
Source Port	
Destination Port	
ICMP Type	

Help

This page will allow you to configure the packet filters for packets received on the WAN interface.

Action: Packets will be dropped or passed (forwarded) if they match the rest of the criteria in this rule. When a field is left blank, that aspect of the rule will match for all packets.

Source IP Address Range: This field accepts either a single IP address, a range of IP addresses in the form "start address - end address", or a range in the form ipaddress/mask, where mask should be of variable length subnet mask format ranging from 0 to 32. If the packet source ip address falls in this range and the rest of the criteria matches, the rule is processed. This field is the IP address of a device on the Internet.

Destination IP Address Range: Specify this field as described above for the Source IP Address Range. This field is the IP address of a LAN device.

Protocol: Packets will be inspected for the specified protocol. If the protocol matches, this rule is processed.

Source Port: Packets will be inspected for the source port if the protocol is TCP or UDP. If the source port matches, this rule is processed.

Destination Port: Packets will be inspected for the destination port if the protocol is TCP or UDP. The the destination port matches, this rule is processed.

ICMP Type: If the protocol is icmp, this field adds another criteria which must match in order for the rule to be processed. ICMP Type is not displayed in the Filter Rule List, but it can be viewed/changed by clicking "Edit".

By default the U-verse RG does not reply to Ping or Trace and does not allow those to be passed thru the firewall from the WAN side.

To enable **Ping and Trace** on the **NVG510** we must use the **Packet Filter** tab in the Firewall.

We would need to change the **Enable Filter** to **On**

We need to then drop down to the **Filter Rule Entry** section and select **Pass**

Then enter the **Source IP** or IP range from which we wish to accept Pings / Traces from – typically the home office or a managing location.

Then enter the **Destination IP Address Range** – again a single IP or and IP range to allow Pings to at this location. Such as the IP of the RG, or a PC or Router / Firewall behind the RG or for Static IP addresses behind the RG.

Then select the **Protocol** – **ICMP** for Ping and Trace.

Source Port and **Destination Port** can be left blank as this is for TCP / UDP traffic not ICMP.

ICMP Type can also be matched

A note about ping and trace –ICMP requests are quite often not answered or answered with a very low priority. Actual data traversing the same hop has a higher priority and does not experience the same delay. So for example in a trace today you may see time outs but the trace completes. The time outs do not indicate a problem but instead indicate only that those hops are configured not to reply to ICMP requests. Also if the destination device is set to not reply then a ping or trace can time out and still not be an accurate indicator of if there is a problem. So keep this in mind.

Configuring Static IP

This Section will walk you through configuring the RG for use of a Static IP block. As mentioned earlier but repeated here for convenience is an overview in differences between ADSL service handling of Static IP service and AT&T U-verse

- **Static IP delivery –**
  - with your DSL service the DSL modem was often set to bridge mode, one IP address was used at the Access device on our side as the Gateway IP address and minus the Network and Broadcast IP addresses the rest were for users to configure on their equipment with the customer device being the next logical hop out from the Access device.
  - With AT&T U-verse the RG is now our access device for this scenario. It has its own IP for its WAN which is a sticky dynamically assigned IP. A Virtual port is then created on the LAN side for the Public / Static IP block and like the DSL Access device uses one IP from the block as the Gateway. The remaining are handed to the customer device.
  - A reason this is different is that the Static IP block is routed to the WAN IP (dynamically assigned) of the RG and mapped to the MAC address of the RG for anti-spoofing purposes.
  - A common misconception is that using DMZplus / IP Passthrough (depending on device) will completely remove the RG as the firewall and the Gateway. Neither of them are the case in general. Those modes pass the sticky DHCP assigned IP of the RG WAN connection, which is separate from the Static IP block , to the assigned device. Also there is always a portion of the RG's firewall functionality that remains in place by design for our U-verse services. This will be discussed in later sections of the document.

Enable Public Routed Sub-interface

This section would have been completed by the U-verse installer and is provided here for reference to verify it is configured as suggested. Also in case of a factory reset where it is required to be reconfigured.

1. **Determine the Public IP block information to configure in the Residential Gateway. (example x.x.x.x /29)**

The RG will use two sets of Public IP addresses, one IP for use between the router and the broadband network (WAN side)and a second independent set of Public Static IP addresses solely for use on the LAN side. The WAN side IP is a Dynamically assigned IP address that is "sticky" It should change only under certain conditions. Some of those conditions are

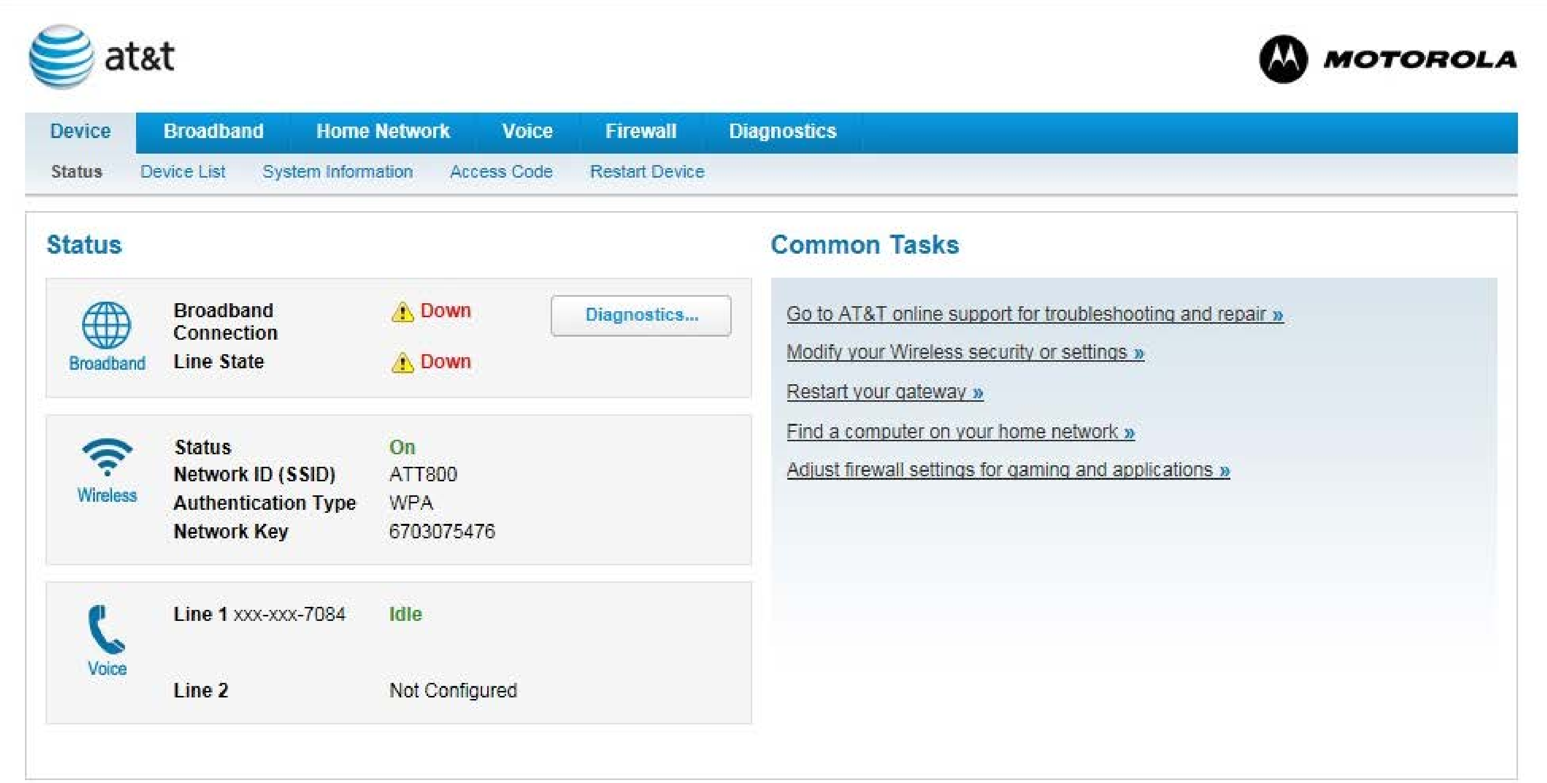
- The RG is swapped
- The VDSL port is swapped at the DSLAM
- The RG is offline for an extended time which could then fail to renegotiate its IP lease.

The Public / Static IP block will be dynamically mapped and routed to the WAN IP and a single IP out of the block will be assigned to a virtual port on the LAN side of the RG. That IP will be the gateway for the rest of the devices using the Static IP block behind the RG. Typically we use the next to last IP in the block for this Gateway IP.

NOTE – if using Cascaded Router config (discussed later) instead of keeping an IP out of the Static IP block to act as a gateway the RG will hand the entire block off to a 3rd party router connected to the Arris RG or modem via private IP, for use on the LAN side of the 3rd party router.

Log into the RG GUI page by putting in the gateway IP (192.168.1.254 is default address and a URL for this is …..)

You should see the opening screen of the portal with something like this.



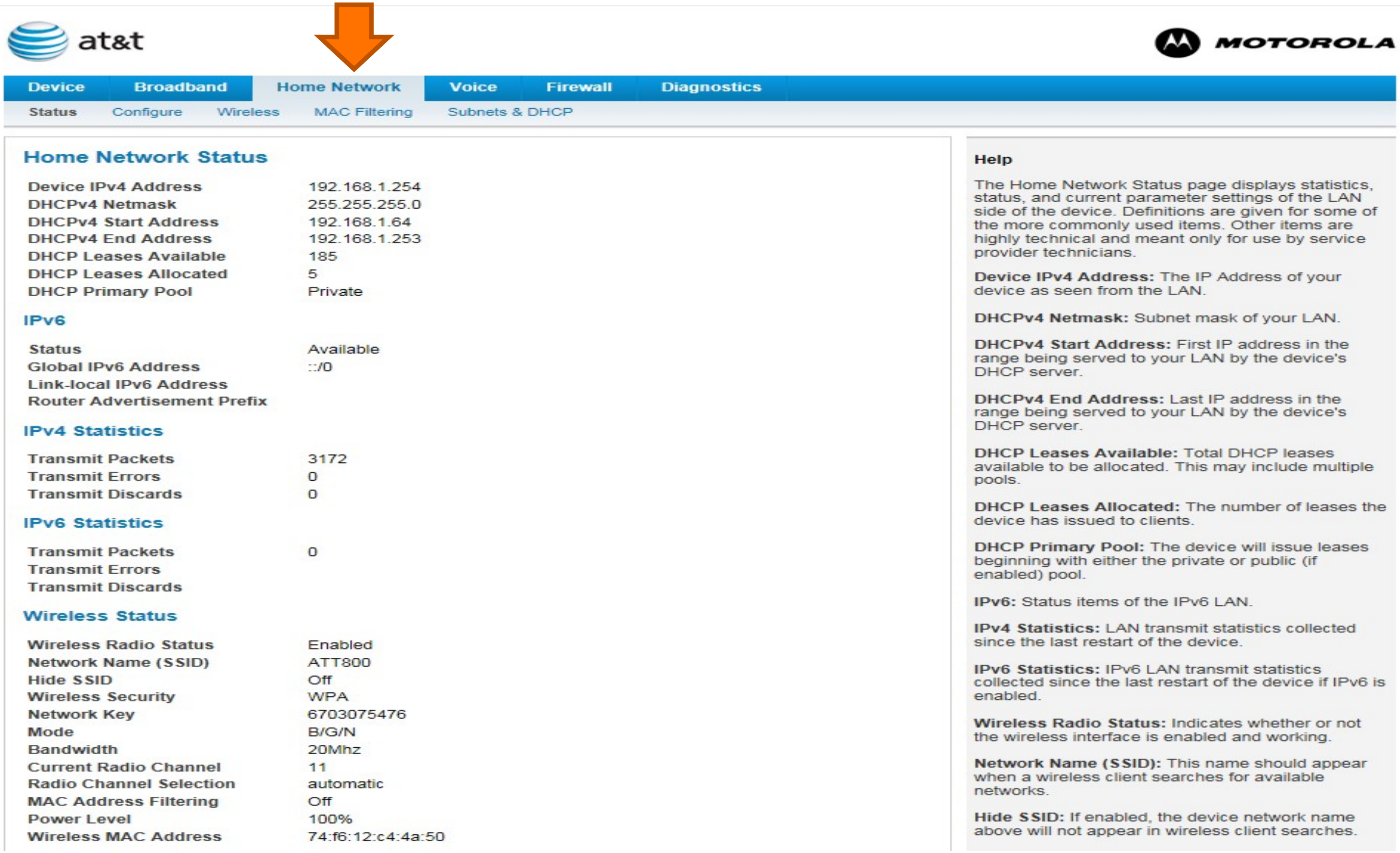
Status

Broadband	Broadband Connection	⚠ Down
	Line State	⚠ Down
Wireless	Status	On
	Network ID (SSID)	ATT800
	Authentication Type	WPA
	Network Key	6703075476
Voice	Line 1 xxx-xxx-7084	Idle
	Line 2	Not Configured

Common Tasks

- Go to AT&T online support for troubleshooting and repair »
- Modify your Wireless security or settings »
- Restart your gateway »
- Find a computer on your home network »
- Adjust firewall settings for gaming and applications »

Click on the Home Network tab which take you to the Status page



Home Network Status

Device IPv4 Address	192.168.1.254
DHCPv4 Netmask	255.255.255.0
DHCPv4 Start Address	192.168.1.64
DHCPv4 End Address	192.168.1.253
DHCP Leases Available	185
DHCP Leases Allocated	5
DHCP Primary Pool	Private

IPv6

Status	Available
Global IPv6 Address	::/0
Link-local IPv6 Address	
Router Advertisement Prefix	

IPv4 Statistics

Transmit Packets	3172
Transmit Errors	0
Transmit Discards	0

IPv6 Statistics

Transmit Packets	0
Transmit Errors	
Transmit Discards	

Wireless Status

Wireless Radio Status	Enabled
Network Name (SSID)	ATT800
Hide SSID	Off
Wireless Security	WPA
Network Key	6703075476
Mode	B/G/N
Bandwidth	20Mhz
Current Radio Channel	11
Radio Channel Selection	automatic
MAC Address Filtering	Off
Power Level	100%
Wireless MAC Address	74:f6:12:c4:4a:50

Help

The Home Network Status page displays statistics, status, and current parameter settings of the LAN side of the device. Definitions are given for some of the more commonly used items. Other items are highly technical and meant only for use by service provider technicians.

Device IPv4 Address: The IP Address of your device as seen from the LAN.

DHCPv4 Netmask: Subnet mask of your LAN.

DHCPv4 Start Address: First IP address in the range being served to your LAN by the device's DHCP server.

DHCPv4 End Address: Last IP address in the range being served to your LAN by the device's DHCP server.

DHCP Leases Available: Total DHCP leases available to be allocated. This may include multiple pools.

DHCP Leases Allocated: The number of leases the device has issued to clients.

DHCP Primary Pool: The device will issue leases beginning with either the private or public (if enabled) pool.

IPv6: Status items of the IPv6 LAN.

IPv4 Statistics: LAN transmit statistics collected since the last restart of the device.

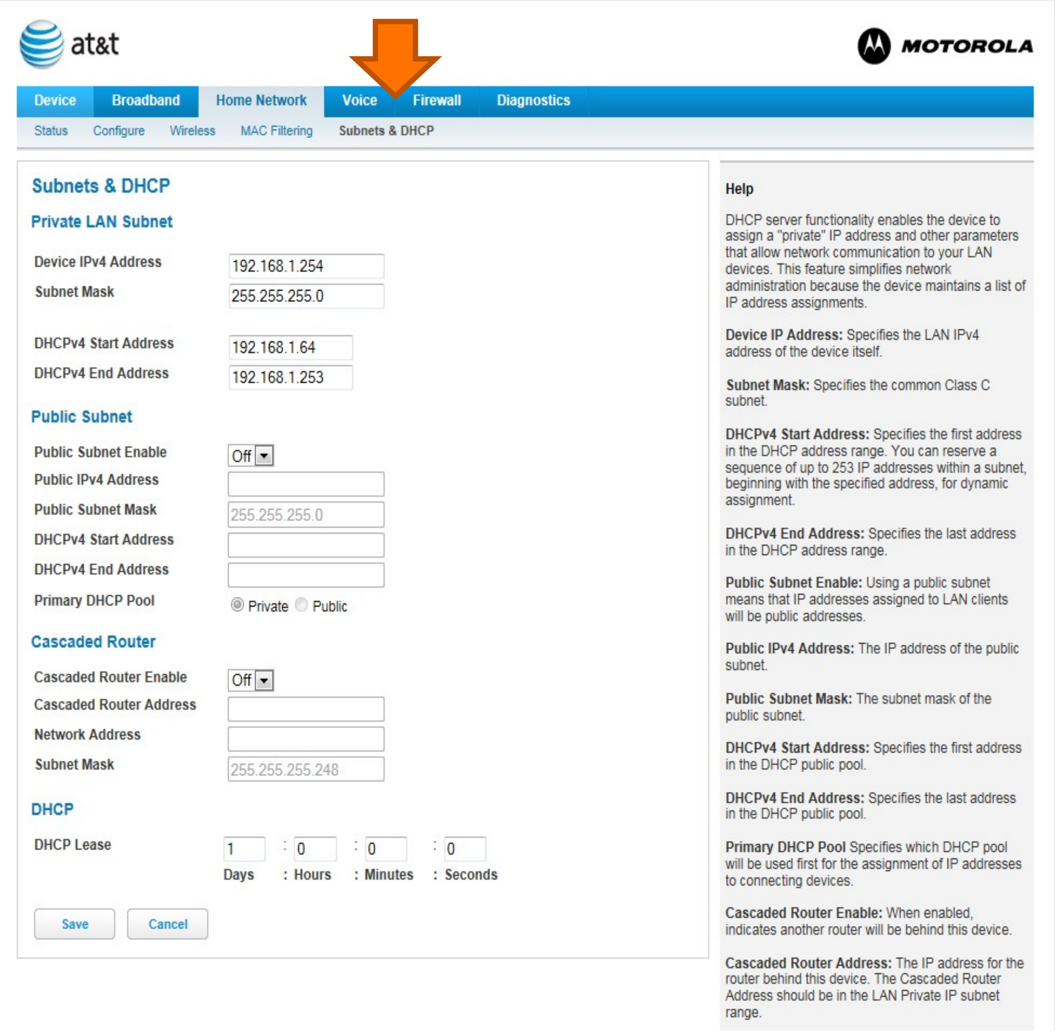
IPv6 Statistics: IPv6 LAN transmit statistics collected since the last restart of the device if IPv6 is enabled.

Wireless Radio Status: Indicates whether or not the wireless interface is enabled and working.

Network Name (SSID): This name should appear when a wireless client searches for available networks.

Hide SSID: If enabled, the device network name above will not appear in wireless client searches.

Click on the Subnets & DHCP sub-tab which take you to this page



Subnets & DHCP

Private LAN Subnet

Device IPv4 Address	192.168.1.254
Subnet Mask	255.255.255.0
DHCPv4 Start Address	192.168.1.64
DHCPv4 End Address	192.168.1.253

Public Subnet

Public Subnet Enable	Off
Public IPv4 Address	
Public Subnet Mask	255.255.255.0
DHCPv4 Start Address	
DHCPv4 End Address	
Primary DHCP Pool	● Private ○ Public

Cascaded Router

Cascaded Router Enable	Off
Cascaded Router Address	
Network Address	
Subnet Mask	255.255.255.248

DHCP

DHCP Lease: 1 Days : 0 Hours : 0 Minutes : 0 Seconds

Help

DHCP server functionality enables the device to assign a "private" IP address and other parameters that allow network communication to your LAN devices. This feature simplifies network administration because the device maintains a list of IP address assignments.

Device IP Address: Specifies the LAN IPv4 address of the device itself.

Subnet Mask: Specifies the common Class C subnet.

DHCPv4 Start Address: Specifies the first address in the DHCP address range. You can reserve a sequence of up to 253 IP addresses within a subnet, beginning with the specified address, for dynamic assignment.

DHCPv4 End Address: Specifies the last address in the DHCP address range.

Public Subnet Enable: Using a public subnet means that IP addresses assigned to LAN clients will be public addresses.

Public IPv4 Address: The IP address of the public subnet.

Public Subnet Mask: The subnet mask of the public subnet.

DHCPv4 Start Address: Specifies the first address in the DHCP public pool.

DHCPv4 End Address: Specifies the last address in the DHCP public pool.

Primary DHCP Pool Specifies which DHCP pool will be used first for the assignment of IP addresses to connecting devices.

Cascaded Router Enable: When enabled, indicates another router will be behind this device.

Cascaded Router Address: The IP address for the router behind this device. The Cascaded Router Address should be in the LAN Private IP subnet range.

Here you will see the **Private LAN subnet** configured.

Below that the **Public Subnet** section. Here is where we will configure your Static IP block for use.

Turn the **Public Subnet Enable** to **On**

Pubic IPv4 Address is the IP the RG will use as the Gateway IP for the rest of your block typically this is the next to last IP in your block.

Public Subnet Mask is in the format of

255.255.255.x with x depending on the number of IP addresses in your block so for 8 Ips this would be 255 – 7 (one less than the number of IP addresses)= 248 so 255.255.255.248

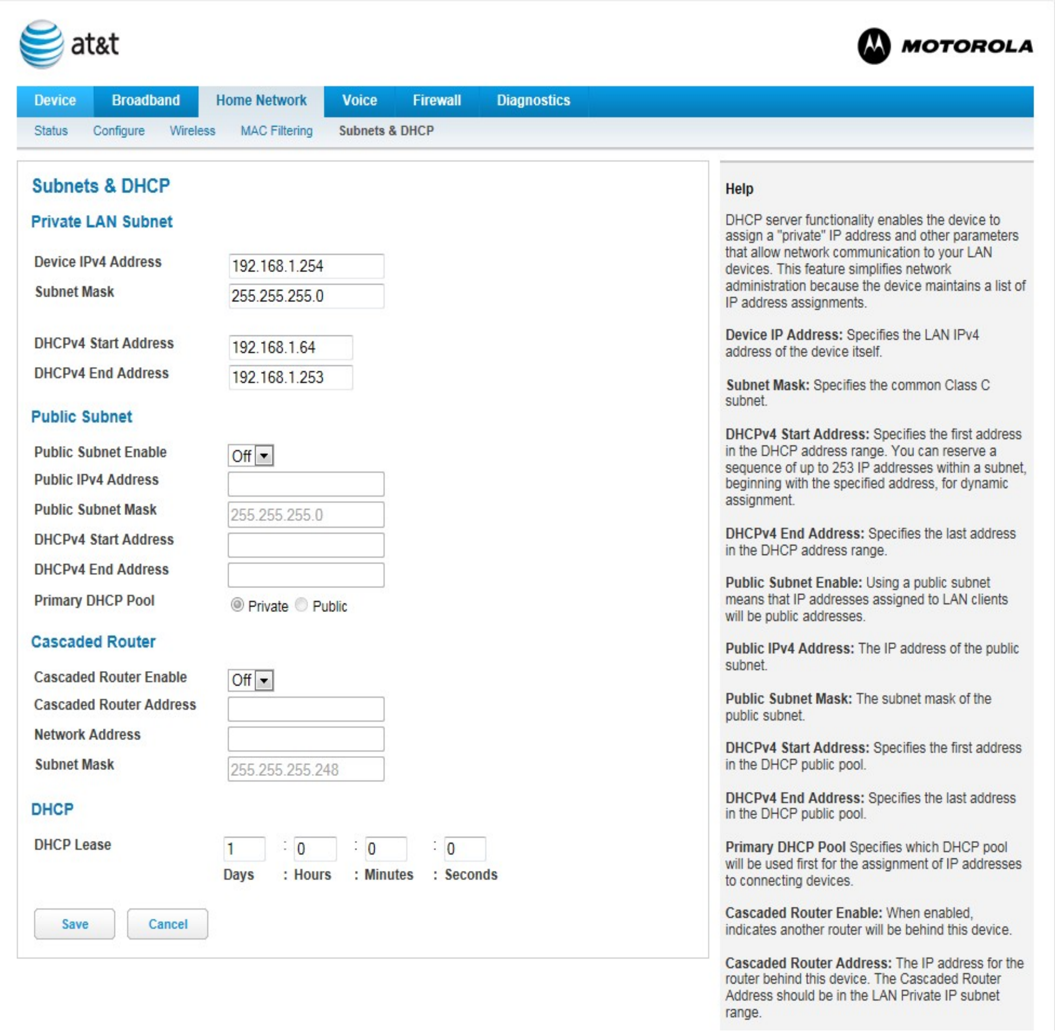
DHCPv4 Start Address is the start address of the usable IP addresses to be assigned.

DHCPv4 End Address would be the last assignable IP which would in our example be one less than the Gateway IP address.

Primary DHCP Pool is to determine which IP pool is default Private pool or Public Pool.

Save

Using Cascaded Router configuration



Subnets & DHCP

Private LAN Subnet

Device IPv4 Address: 192.168.1.254
Subnet Mask: 255.255.255.0

DHCPv4 Start Address: 192.168.1.64
DHCPv4 End Address: 192.168.1.253

Public Subnet

Public Subnet Enable: Off
Public IPv4 Address:
Public Subnet Mask: 255.255.255.0
DHCPv4 Start Address:
DHCPv4 End Address:
Primary DHCP Pool: ● Private ○ Public

Cascaded Router

Cascaded Router Enable: Off
Cascaded Router Address:
Network Address:
Subnet Mask: 255.255.255.248

DHCP

DHCP Lease: 1 Days : 0 Hours : 0 Minutes : 0 Seconds

Help

DHCP server functionality enables the device to assign a "private" IP address and other parameters that allow network communication to your LAN devices. This feature simplifies network administration because the device maintains a list of IP address assignments.

Device IP Address: Specifies the LAN IPv4 address of the device itself.

Subnet Mask: Specifies the common Class C subnet.

DHCPv4 Start Address: Specifies the first address in the DHCP address range. You can reserve a sequence of up to 253 IP addresses within a subnet, beginning with the specified address, for dynamic assignment.

DHCPv4 End Address: Specifies the last address in the DHCP address range.

Public Subnet Enable: Using a public subnet means that IP addresses assigned to LAN clients will be public addresses.

Public IPv4 Address: The IP address of the public subnet.

Public Subnet Mask: The subnet mask of the public subnet.

DHCPv4 Start Address: Specifies the first address in the DHCP public pool.

DHCPv4 End Address: Specifies the last address in the DHCP public pool.

Primary DHCP Pool Specifies which DHCP pool will be used first for the assignment of IP addresses to connecting devices.

Cascaded Router Enable: When enabled, indicates another router will be behind this device.

Cascaded Router Address: The IP address for the router behind this device. The Cascaded Router Address should be in the LAN Private IP subnet range.

Cascaded Router mode should only be used by Advanced users who understand the implications.

Cascaded Router will as stated earlier, hand the entire Static IP block to a 3rd party router for it to handle the routing and IP assignments of the block.

That router will be connected to the RG using a private IP, which means that the Static IP block will be NAT'ed from the 3rd party router out to the RG or modem and the Internet.

Cascaded Router and **Public Subnet** configuration can not both be enabled.

Cascaded Router Enable – set to **On**

Cascaded Router Address – the private IP of the 3rd Party router that you will hand off and configure the Static IP block on

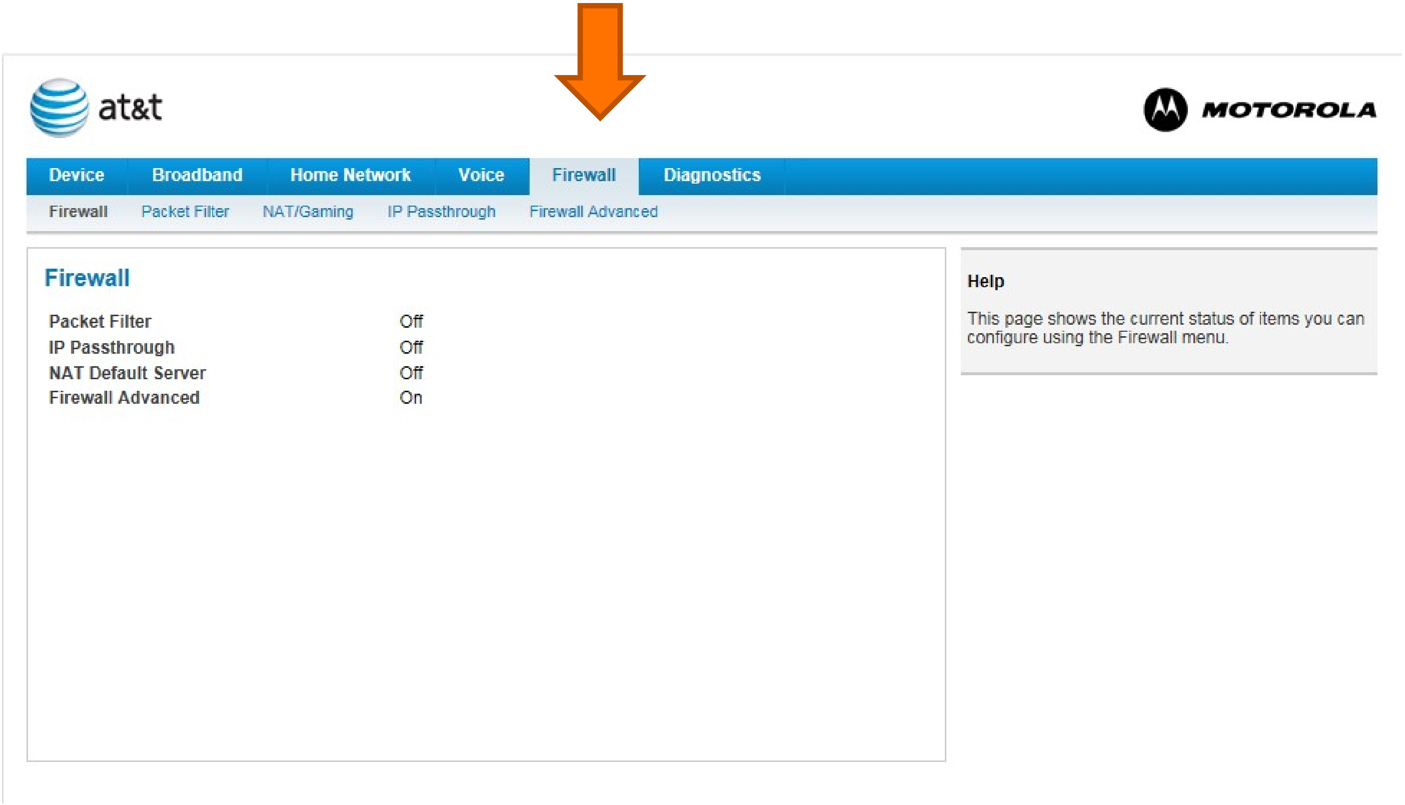
Network Address is the starting IP of the Static IP block

Subnet Mask is the subnet mask that matches the Static IP block (255.255.255.248 if 8 IPs)

Save

Configuring for IP Passthrough mode

Click on the Firewall tab.



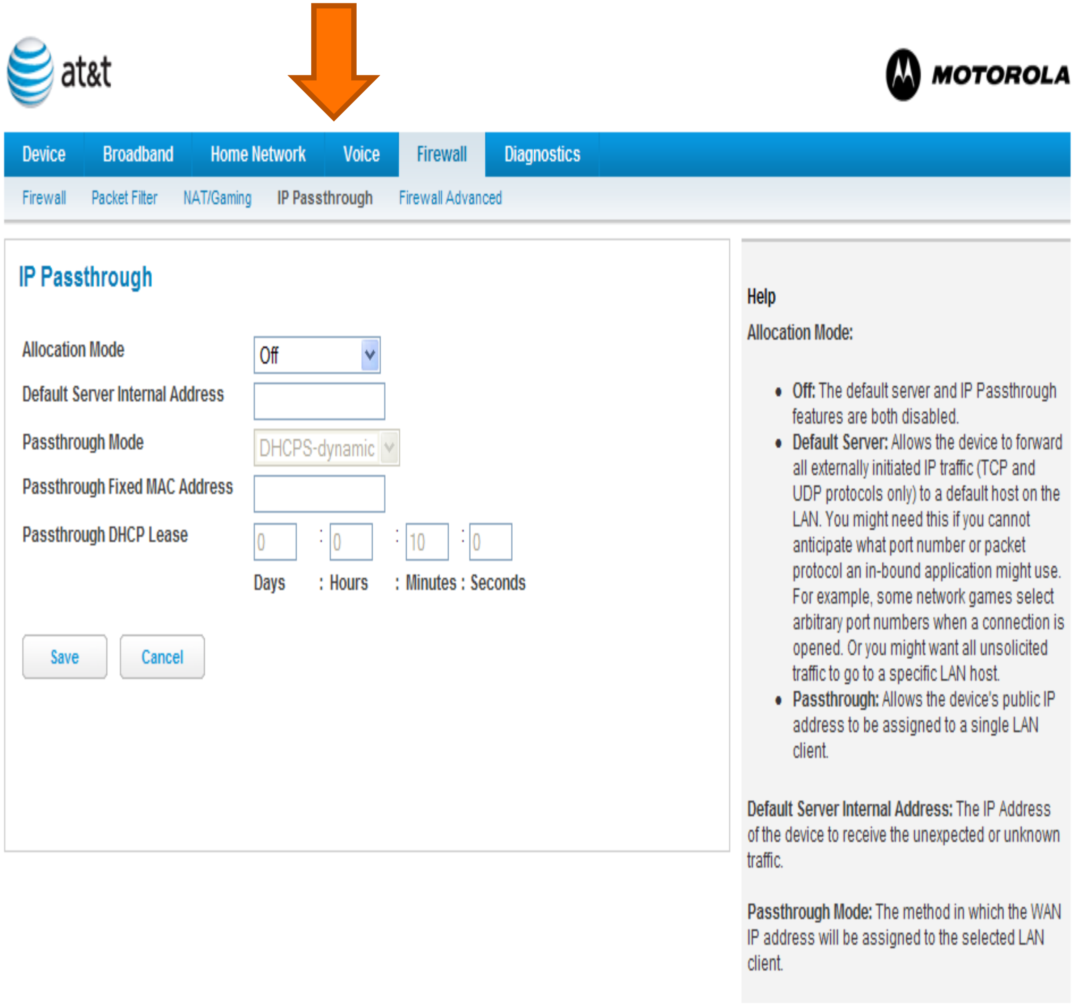
Firewall

Packet Filter	Off
IP Passthrough	Off
NAT Default Server	Off
Firewall Advanced	On

Help

This page shows the current status of items you can configure using the Firewall menu.

Click on the IP Passthrough sub-tab



IP Passthrough

Allocation Mode	Off
Default Server Internal Address	
Passthrough Mode	DHCPS-dynamic
Passthrough Fixed MAC Address	
Passthrough DHCP Lease	0 : 0 : 10 : 0 Days : Hours : Minutes : Seconds

Help

Allocation Mode:

- **Off:** The default server and IP Passthrough features are both disabled.
- **Default Server:** Allows the device to forward all externally initiated IP traffic (TCP and UDP protocols only) to a default host on the LAN. You might need this if you cannot anticipate what port number or packet protocol an in-bound application might use. For example, some network games select arbitrary port numbers when a connection is opened. Or you might want all unsolicited traffic to go to a specific LAN host.
- **Passthrough:** Allows the device's public IP address to be assigned to a single LAN client.

Default Server Internal Address: The IP Address of the device to receive the unexpected or unknown traffic.

Passthrough Mode: The method in which the WAN IP address will be assigned to the selected LAN client.

IP Passthough will share the **WAN IP** of the **RG or modem** to the specific device. It will not be one of the **Static IP's** assigned if you have those. It will not completely bypass the firewall but for most uses it will and in many cases you can add pinhole rules for any that may not work as expected while in this mode.

Allocation Mode – set to **Passthrough**

Default Server Internal Address – not used for **Passthrough** mode

Passthrough Mode – by default this is set to **DHCPS-dynamic.**

Passthrough Fixed MAC Address – the **MAC Address** of the device to be used in **Passthrough mode**

Passthrough DHCP Lease – if you wish to modify the lease time.

Save

IP Passthrough may be enabled along with Cascade Router.